GroupWise 18

Administration Guide

November 2017

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.

Copyright © 2017 Micro Focus Software Inc. All Rights Reserved.

Contents

About This Guide **29**

Part I System **31**

1 GroupWise System Administration **33**

2 GroupWise Administration Console **35**

Accessing the GroupWise Admin Console 35
Connecting to a Domain 35
Understanding the Need for Domain Connections 35
Selecting a Domain 36
Getting Acquainted with the GroupWise Admin Console 36
Monitoring Background Administrative Tasks 36
Managing the GroupWise Admin Service 36
Linux: Managing the GroupWise Admin Service 37
Windows: Managing the GroupWise Admin Service 38
Using the GroupWise Administration Utility 39
Using an LDAP Directory Management Tool for Adding LDAP Users and Groups to GroupWise 40
Adding GroupWise Users and Groups in Micro Focus iManager 40
Managing GroupWise Users and Groups in Microsoft Management Console 42

3 GroupWise Administrators **45**

Managing the GroupWise Super Admin User 45
Designating Additional GroupWise System Administrators 46
Designating Domain Administrators 46
Designating Post Office Administrators 46
Designating a Specific User as an Administrator 47

4 GroupWise System Tools **49**

Addressing Rules 50
Admin-Defined Fields 50
Administrators 51
Calendar Publishing 51
Directory Associations 51
Document Viewer Agent 51
Email Address Lookup 51
Expired Records 51
External System Synchronization 51
Global Signatures 52
Information 52
Internet Addressing 52
LDAP Directories and Servers 52
Licensing 52
Automatically Configure License 53
Manually Configure License 53

Legacy 53
Link Configuration 54
Pending Operations 54
Record Enumerations 55
Recover Deleted Account 55
Restore Area Management 55
System Preferences 56
Admin Preferences 57
Routing Options 58
External Access Rights 58
Nickname Settings 59
Default Password 59
Admin Lockout Settings 60
Archive Service Settings 60
Time Zones 61
Modifying a Time Zone Definition 62
Adding a Time Zone Definition 63
Deleting a Time Zone Definition 64
Trusted Applications 64
Creating a Trusted Application and Key 65
Editing a Trusted Application 66
Deleting a Trusted Application 67
User Import 67
User Move Status 67
Standalone GroupWise Database Utilities 67
GroupWise Check Utility (GWCheck) 68
GroupWise Backup Time Stamp Utility (GWTMSTMP) 68
GroupWise Administration Utility (GWAdminUtil) 68
GroupWise Database Copy Utility (DBCOPY) 68

5 GroupWise Address Book 69

Customizing Address Book Fields 69
Adding LDAP Fields to the Address Book 70
Changing the Default Sort Order 71
Changing the Default Field Order 71
Removing Fields from the Address Book 71
Preventing the User Description Field from Displaying in the Address Book 72
Controlling Object Visibility 72
Updating Address Book Information 73
Synchronizing Information 73
Rebuilding the Post Office Database 74
Controlling Users’ Frequent Contacts Address Books 74
Controlling Address Book Synchronization for Caching and Remote Client Users 75
Publishing Email Addresses to the LDAP Directory 76
Enabling Wildcard Addressing 76
Setting Wildcard Addressing Levels 77
Wildcard Addressing Syntax 77
Adding External Users to the GroupWise Address Book 78

6 LDAP Directories and Servers in Your GroupWise System 79

Setting Up an LDAP Directory 79
Creating the LDAP Directory Object 80
Configuring User Synchronization for an LDAP Directory 80
Configuring LDAP Authentication 81
Enabling Email Publishing 81

Setting Up an LDAP Server 81
Adding an LDAP Server 82
Configuring a Pool of LDAP Servers 83
Specifying Failover LDAP Servers (Non-SSL Only) 83

7 Multilingual GroupWise Systems 85

GroupWise User Languages 85
GroupWise Client Languages 85
GroupWise Spell Checker Languages 86
GroupWise Administration and Agent Languages 87
International Character Considerations 88
MIME Encoding 88
Multi-Language Workstations 89

Part II Domains 91

8 Creating a New Domain 93

Understanding the Purpose of Domains 93
Creating a New Domain on a New Domain Server 94
Creating a New Domain on an Existing Domain Server 94
What’s Next 94

9 Managing Domains 95

Connecting to a Domain 95
Editing Domain Properties 95
Converting a Secondary Domain to a Primary Domain 96
Deleting a Domain 96
Changing the MTA Configuration to Meet Domain Needs 97
Releasing a Domain from Your GroupWise System 97
Merging a Domain into Your GroupWise System 98

10 Managing the Links between Domains and Post Offices 101

Understanding Link Configuration 101
Domain-to-Domain Links 101
Domain-to-Post-Office Links 104
Link Protocols for Direct Links 104
Using the Link Configuration Tool 106
Accessing the Link Configuration Tool 106
Editing Domain Links 107

11 Using an External Domain to Represent Another Email System 109

Using a Non-GroupWise Domain to Represent the Internet 109
Creating a Non-GroupWise Domain to Represent an Email System across the Internet 109
Linking to the Non-GroupWise Domain 110
Creating an External Post Office to Represent an Internet Host 110
Creating External Users to Represent Internet Users 111
Configuring External Users and Resources to Appear in GroupWise Busy Searches 112
Using an External Domain to Connect GroupWise Systems 112
GroupWise System Connection Overview 112
Creating an External Domain 113

Linking to the External Domain . . . 113
Synchronizing User Information between External GroupWise Systems . . . 115

Part III Post Offices 117

12 Creating a New Post Office 119

Understanding the Purpose of Post Offices . . . 119
Creating a New Post Office on a New Post Office Server . . . 120
Creating a New Post Office on an Existing Domain or Post Office Server . . . 120
What's Next . . . 120

13 Managing Post Offices 121

Connecting to the Domain That Owns a Post Office . . . 121
Editing Post Office Properties . . . 121
Managing Disk Space Usage in the Post Office . . . 121
Understanding Disk Space Usage and Mailbox Size Limits . . . 122
Preparing to Implement Disk Space Management . . . 123
Setting Mailbox Size Limits . . . 123
Enforcing Mailbox Size Limits . . . 124
Restricting the Size of Messages That Users Can Send . . . 125
Preventing the Post Office from Running Out of Disk Space . . . 126
An Alternative to Disk Space Management in the Post Office . . . 127
Forcing Caching Mode . . . 127
Auditing Mailbox License Usage in the Post Office . . . 127
Viewing Current Client Usage in the Post Office . . . 129
Restricting Client Access to the Post Office . . . 129
Securing the Post Office with LDAP Authentication . . . 130
Disabling a Post Office . . . 130
Deleting a Post Office . . . 131
Changing POA Configuration to Meet Post Office Needs . . . 131

Part IV Post Office Agent 133

14 Understanding Message Delivery and Storage in the Post Office 135

The Post Office and the POA in Your GroupWise System . . . 135
Post Office and POA Representation in the GroupWise Admin Console . . . 135
Information Stored in the Post Office . . . 135
Post Office Database . . . 136
Message Store . . . 136
Guardian Database . . . 137
Agent Input/Output Queues in the Post Office . . . 138
Libraries (optional) . . . 138
Role of the Post Office Agent . . . 139
Client/Server Processing . . . 139
Message File Processing . . . 140
Other POA Functions . . . 140

15 Configuring the POA 143

Performing Basic POA Configuration . . . 143
Creating a New POA in the GroupWise Admin Console . . . 144
Configuring the POA in the GroupWise Admin Console . . . 144

Binding the POA to a Specific IP Address . . . 144
Configuring the POA for Remote Server Login (Windows Only) . . . 145
Configuring User Access to the Post Office . . . 145
Simplifying Client Access with a GroupWise Name Server . . . 145
Supporting IMAP Clients . . . 147
Supporting SOAP Clients . . . 148
Checking What GroupWise Clients Are in Use . . . 148
Supporting Forced Mailbox Caching . . . 149
Restricting Message Size between Post Offices . . . 149
Supporting Calendar Publishing . . . 150
Configuring Post Office Security . . . 150
Securing Client Access through an External Proxy Server . . . 150
Controlling Client Redirection Inside and Outside Your Firewall . . . 151
Securing the Post Office with SSL Connections to the POA . . . 152
Providing LDAP Authentication for GroupWise Users . . . 153
Configuring Intruder Detection . . . 153
Configuring Trusted Application Support . . . 154
Configuring Post Office Maintenance . . . 154
Scheduling Database Maintenance . . . 154
Scheduling Disk Space Management . . . 156
Configuring Nightly User Upkeep . . . 157

16 Managing the POA 159

Configuring the POA Console . . . 159
Accessing the POA Console . . . 160
Changing POA Configuration Settings . . . 160
Controlling the POA MTP Threads . . . 160
Disconnecting a User Session from the POA . . . 161

17 Monitoring the POA 163

Using the POA Console . . . 163
Monitoring POA Status . . . 163
Monitoring POA Threads . . . 163
Tracking Peak Values for Connections, Queue Contents, and Thread Usage . . . 163
Listing POA Scheduled Events . . . 164
Checking Link Status to the MTA . . . 164
Taking Performance Snapshots . . . 164
Monitoring SOAP Events . . . 165
Using POA Log Files . . . 166
Locating POA Log Files . . . 166
Configuring POA Log Settings and Switches . . . 167
Viewing and Searching POA Log Files . . . 167
Interpreting POA Log File Information . . . 168
Using GroupWise Monitor . . . 168
Using Micro Focus Remote Manager . . . 168
Using an SNMP Management Console . . . 168
Setting Up SNMP Services for the POA . . . 168
Copying and Compiling the POA MIB File . . . 169
Configuring the POA for SNMP Monitoring . . . 170

18 Optimizing the POA 171

Optimizing Client/Server Processing . . . 171
Adjusting the Number of Client/Server Threads . . . 171
Adjusting the Number of Client/Server Connections . . . 172
Optimizing Thread Management . . . 172

Optimizing Message File Processing 173
Optimizing Database Maintenance 174
Optimizing Client Purge Operations 174
Optimizing Calendar Publishing 175

19 Managing Indexing of Attachment Content 177

Configuring Indexing 177
Controlling Indexing 178
Configuring the POA with Multiple DVAs for Indexing 178
Controlling Maximum Document Conversion Size and Time 179
Customizing Indexing 179
    Determining What to Index 179
    Determining Indexing Priority 180
    Reclaiming Disk Space 180
    Preventing Indexing of Specific Document Types 181

20 Using POA Startup Switches 183

@startup_file_name 186
--adminport 187
--attemptsresetinterval 187
--certfile 187
--cluster 187
--dhparm 188
--dvafilter 188
--dva*n*ipaddr 188
--dva*n*port 189
--dva*n*ssl 189
--dvamaxsize 189
--dvamaxtime 190
--dvaquarantine 190
--enforceclientversion 190
--evocontrol 191
--externalclientssl 191
--gwchkthreads 191
--gwclientreleasedate 192
--gwclientreleaseversion 192
--help 192
--home 192
--httppassword 193
--httpport 193
--httprefresh 193
--httpssl 194
--httpuser 194
--imap 194
--imapmaxthreads 195
--imapreadlimit 195
--imapreadnew 195
--imapport 195
--imapssl 196
--imapsslport 196
--incorrectloginattempts 196
--internalclientssl 197

--intruderlockout . . . 197
--ip . . . 197
--keyfile . . . 198
--keypassword . . . 198
--language . . . 198
--ldapdisablepwdchg . . . 199
--ldapipaddr . . . 199
--ldappoolresettime . . . 199
--ldapport . . . 200
--ldappwd . . . 200
--ldapssl . . . 200
--ldapsslkey . . . 200
--ldaptimeout . . . 201
--ldapuser . . . 201
--ldapuserauthmethod . . . 201
--lockoutresetinterval . . . 202
--log . . . 202
--logdays . . . 203
--logdiskoff . . . 203
--loglevel . . . 203
--logmax . . . 204
--maxappconns . . . 204
--maxphysconns . . . 204
--mtpinipaddr . . . 205
--mtpinport . . . 205
--mtpoutipaddr . . . 205
--mtpoutport . . . 205
--mtpsendmax . . . 206
--mtpssl . . . 206
--name . . . 206
--noada . . . 207
--nocache . . . 207
--noconfig . . . 207
--noerrormail . . . 207
--nogwchk . . . 208
--nomf . . . 208
--nomfhigh . . . 208
--nomflow . . . 208
--nomtp . . . 209
--nonuu . . . 209
--noqf . . . 209
--nordab . . . 209
--norecover . . . 210
--nosnmp . . . 210
--notcpip . . . 210
--nuuoffset . . . 210
--password . . . 211
--peakrefreshinterval . . . 211
--port . . . 211
--primingmax . . . 211
--qfbaseoffset . . . 212
--qfbaseoffsetinminute . . . 212
--qfdeleteold . . . 212

--qfinterval 213
--qfintervalinminute 213
--qflevel 213
--qfnolibs 214
--qfnopreproc 214
--qfnousers 214
--qfuserfidbeg 215
--qfuserfidend 215
--rdaboffset 215
--rights 216
--show 216
--soap 216
--soapmaxthreads 216
--soapport 217
--soapsizelimit 217
--soapssl 217
--soapthreads 218
--sslciphersuite 218
--ssloption 218
--tcpthreads 218
--threads 219
--user 219

Part V Message Transfer Agent 221

21 Understanding Message Transfer between Domains and Post Offices 223

The Domain and the MTA in Your GroupWise System 223
Domain and MTA Representation in the GroupWise Admin Console 223
Information Stored in the Domain 223
Domain Database 224
Agent Input/Output Queues in the Domain 224
Role of the Message Transfer Agent 225
Link Configuration between Domains and Post Offices 225

22 Configuring the MTA 227

Performing Basic MTA Configuration 227
Creating an MTA Object in the GroupWise Admin Console 227
Configuring the MTA in the GroupWise Admin Console 227
Binding the MTA to a Specific IP Address 228
Enabling MTA Message Logging 228
Configuring Domain Access 229
Securing the Domain with SSL Connections to the MTA 229
Restricting Message Size between Domains 230
Configuring a Routing Domain 231
Configuring User Synchronization 232
Configuring LDAP User Synchronization 232
Configuring Exchange Address Book Synchronization 233
Configuring the LDAP Server Capabilities 233

23 Managing the MTA 235

Setting Up the MTA Console 235
Accessing the MTA Console 235

Changing MTA Configuration Settings . . . 236
Controlling Links to Other Locations . . . 236

24 Monitoring the MTA 237

Using the MTA Console. . . . 237
Monitoring MTA Status . . . 237
Monitoring the Routing Queue . . . 237
Monitoring Links . . . 237
Tracking Messages . . . 238
Using MTA Log Files . . . 238
Locating MTA Log Files . . . 238
Configuring MTA Log Settings and Switches . . . 238
Viewing and Searching MTA Log Files. . . . 239
Interpreting MTA Log File Information . . . 240
Using GroupWise Monitor . . . 240
Using Micro Focus Remote Manager . . . 240
Using an SNMP Management Console . . . 240
Setting Up SNMP Services for the MTA. . . . 240
Copying and Compiling the MTA MIB File . . . 241
Configuring the MTA for SNMP Monitoring . . . 242
Receiving Notifications of Agent Problems . . . 242
Using MTA Message Logging . . . 242

25 Optimizing the MTA 243

Optimizing TCP/IP Links . . . 243
Adjusting the Number of MTA TCP/IP Connections . . . 243
Adjusting the MTA Wait Intervals for Slow TCP/IP Connections . . . 243
Optimizing the Routing Queue . . . 244
Adjusting the Maximum Number of Active Router Threads . . . 244
Adjusting the Maximum Number of Idle Router Threads . . . 244
Adjusting MTA Polling of Closed Locations. . . . 244

26 Using MTA Startup Switches 247

@startup_file_name . . . 249
--activelog . . . 249
--adminport . . . 249
--certfile . . . 249
--cluster . . . 250
--cyhi . . . 250
--cylo . . . 250
--defaultroutingdomain . . . 250
--dhparm . . . 251
--fast0 . . . 251
--fast4 . . . 251
--help . . . 251
--home. . . . 252
--httppassword . . . 252
--httpport . . . 252
--httprefresh . . . 253
--httpssl . . . 253
--httpuser. . . . 253
--ip . . . 253

--keyfile . . . 254
--keypassword . . . 254
--language . . . 254
--log . . . 255
--logdays . . . 255
--logdiskoff . . . 255
--loglevel . . . 256
--logmax . . . 256
--maxidlerouters . . . 256
--maxrouters . . . 257
--messagelogdays . . . 257
--messagelogmaxsize . . . 257
--messagelogpath . . . 257
--messagelogsettings . . . 258
--msgtranssl . . . 258
--noada . . . 258
--nodns . . . 258
--noerrormail . . . 259
--nondssync . . . 259
--norecover . . . 259
--nosnmp . . . 259
--show . . . 259
--sslciphersuite . . . 260
--ssloption . . . 260
--tcpinbound . . . 260
--tcpport . . . 261
--tcpwaitconnect . . . 261
--tcpwaitdata . . . 261
--vsnoadm . . . 262
--work . . . 262

Part VI Internet Agent 263

27 Understanding Message Transfer to and from the Internet 265

The GWIA in Your GroupWise System . . . 265
GWIA Representation in the GroupWise Admin Console . . . 265
Services Provided by the GWIA . . . 265

28 Configuring the GWIA 269

Creating a New GWIA in the GroupWise Admin Console . . . 269
Configuring the GWIA in the GroupWise Admin Console . . . 270
Configuring an Alternate GWIA for a Domain . . . 270
Binding the GWIA to a Specific IP Address . . . 270
Securing Internet Access with SSL Connections to the GWIA . . . 271
Deleting a GWIA . . . 272

29 Managing Internet Domains, Addressing, and Access 273

Planning GWIAs Used for Outbound Messages . . . 273
Planning Internet Domain Names . . . 273
Understanding Internet Addressing Formats . . . 274

Preferred Address Format 274
Allowed Address Formats 276
Configuring Internet Addressing 277
Adding Internet Domain Names 277
Establishing Default GWIAs for Domains 277
Changing the Preferred and Allowed Address Formats for Your GroupWise System 278
Overriding Internet Addressing 278
Setting a Preferred Email ID 279
Managing Internet Access 279
Controlling User Access to the Internet 279
Blocking Unwanted Email from the Internet 285
Tracking Internet Traffic with Accounting Data 290

30 Configuring SMTP/MIME Services 293

Configuring Basic SMTP/MIME Settings 293
Using Extended SMTP (ESMTP) Options 295
Configuring How the GWIA Handles Email Addresses 296
Determining Format Options for Messages 298
Configuring the SMTP Timeout Settings 299
Determining What to Do with Undeliverable Messages 300
Enabling SMTP Relaying 300
Using a Route Configuration File 301
Customizing Delivery Status Notifications 302
Managing MIME Messages 303
Customizing MIME Preamble Text 303
Customizing MIME Content-Type Mappings 304

31 Configuring POP3/IMAP4 Services 307

Enabling POP3/IMAP4 Services 307
Configuring Post Office Links 308
Giving POP3 or IMAP4 Access Rights to Users 308
Setting Up an Email Client for POP3/IMAP4 Services 308
User Name Login Options 309

32 Monitoring the GWIA 311

Using the GWIA Console 311
Setting Up the GWIA Console 311
Accessing the GWIA Console 312
Using GWIA Log Files 312
Locating GWIA Log Files 312
Configuring GWIA Log Settings and Switches 312
Viewing and Searching Log Files 313
Using GroupWise Monitor 313
Using Micro Focus Remote Manager 313
Using an SNMP Management Console 313
Setting Up SNMP Services for the GWIA 314
Copying and Compiling the GWIA MIB File 315
Configuring the GWIA for SNMP Monitoring 315
Assigning Users to Receive GWIA Warning and Error Messages 315
Stopping the GWIA 316
Using a Mail Message 316
Using a Shutdown File 316

33 Optimizing the GWIA 317

Optimizing Send/Receive Threads . . . 317
Increasing Polling Time . . . 317
Decreasing the Timeout Cycles . . . 318

34 Using GWIA Startup Switches 319

Alphabetical List of Switches . . . 319
Required Switches . . . 324
@config_file_name . . . 325
--dhome . . . 325
--hn . . . 325
--home . . . 325
Environment Switches . . . 325
--cluster . . . 326
--ip . . . 326
--ipa . . . 326
--ipp . . . 326
--nosnmp . . . 326
--smtphome . . . 327
--work . . . 327
--nasoq . . . 327
SMTP/MIME Switches . . . 327
SMTP Enabled . . . 328
iCal Enabled . . . 328
Address Handling . . . 328
Message Formatting and Encoding . . . 333
Forwarded and Deferred Messages . . . 337
Extended SMTP . . . 338
Send/Receive Cycle and Threads . . . 339
Dial-Up Connections . . . 340
Timeouts . . . 341
Relay Host . . . 342
Host Authentication . . . 342
Undeliverable Message Handling . . . 343
Mailbomb and Spam Security . . . 344
POP3 Switches . . . 345
--nopopversion . . . 346
--pop3 . . . 346
--popintruderdetect . . . 346
--popport . . . 346
--popsport . . . 346
--popssl . . . 346
--pt . . . 347
--sslpt . . . 347
IMAP4 Switches . . . 347
--imap4 . . . 347
--imapport . . . 348
--imapreadlimit . . . 348
--imapreadnew . . . 348
--imapsport . . . 348
--imapssl . . . 348
--it . . . 349
--noimapversion . . . 349
--sslit . . . 349
SSL Switches . . . 349
--certfile . . . 350
--dhparm . . . 350

--keyfile 350
--keypasswd 350
--smtpssl 350
--httpssl 351
--popssl 351
--imapssl 351
/ldapssl 351
--sslciphersuite 352
--ssloption 352
LDAP Switches 352
GroupWise Authentication Switches 352
LDAP Query Switches 353
Log File Switches 355
--log 355
--logdays 355
--loglevel 355
--logmax 356
Console Switches (HTTP) 356
--httpport 356
--httpuser 356
--httppassword 357
--httprefresh 357
--httpssl 357
Console Switches (Server) 357
--color 357
--help 357
--mono 358
--show (Linux Only) 358

Part VII Document Viewer Agent **359**

35 Understanding Document Conversion **361**

36 Scaling Your DVA Installation **363**

DVA Configurations 363
Basic DVA Installation 363
Multiple DVAs for a Post Office 364
Multiple DVAs for WebAccess 364
Multiple Shared DVAs 365
Installing the DVA 365
Linux: Installing and Starting the DVA 365
Windows: Installing and Starting a New DVA 366
Setting Up the DVA 367
Creating a DVA Object 367
Adding a DVA to a POA 367

37 Configuring the DVA **369**

Editing the startup.dva File 369
Setting the DVA Home Folder 369
Changing the DVA IP Address or Port Number 370
Securing Document Conversion with SSL Connections 371
Enabling the DVA Document Quarantine 371
Putting DVA Configuration Changes into Effect 372
Linux: Stopping and Starting the DVA 372
Windows: Stopping and Starting the DVA 372

38 Monitoring the DVA 373

Using the DVA Console . . . 373
Configuring the DVA Console . . . 373
Viewing the DVA Console . . . 373
Using DVA Log Files . . . 374
Locating DVA Log Files . . . 374
Configuring DVA Log Settings . . . 374
Viewing DVA Log Files . . . 375
Interpreting DVA Log File Information . . . 375

39 Optimizing the DVA 377

Controlling Thread Usage . . . 377
Controlling Maximum Document Conversion Size and Time Limits . . . 377

40 Using DVA Startup Switches 379

@startup_file_name . . . 380
--cleanTmpInterval . . . 380
--dhparm . . . 380
--home . . . 381
--httpmaxthread . . . 381
--httpport . . . 382
--httppassword . . . 382
--httpssl . . . 382
--httpthread . . . 382
--httpuser . . . 383
--ip . . . 383
--log . . . 383
--logdays . . . 384
--loglevel . . . 384
--logmax . . . 384
--maxquarantineage . . . 385
--maxquarantinesize . . . 385
--maxtime . . . 385
--PDFSizeThreshold . . . 386
--PDFReturnNoImage . . . 386
--quarantine . . . 386
--sslcert . . . 386
--sslciphersuite . . . 387
--sslkey . . . 387
--sslkeypassword . . . 387
--ssloption . . . 388

Part VIII Databases 389

41 Understanding GroupWise Databases 391

Domain Databases . . . 391
Post Office Databases . . . 391
User Databases . . . 392
Message Databases . . . 392
Library Databases . . . 392

Guardian Databases . . . 393

42 Maintaining Domain and Post Office Databases 395

Validating Domain or Post Office Databases . . . 395
Recovering Domain or Post Office Databases . . . 396
Rebuilding Domain or Post Office Databases . . . 398
Replacing the Primary Domain Database with a Secondary Domain Database . . . 400
Rebuilding Database Indexes . . . 401

43 Maintaining User/Resource and Message Databases 403

Recovering User/Resource and Message Databases . . . 403
Analyzing and Fixing User/Resource and Message Databases . . . 403
Performing a Structural Rebuild of a User/Resource Database . . . 405
Re-creating a User/Resource Database . . . 406

44 Maintaining Library Databases and Documents 407

Analyzing and Fixing Databases for Libraries and Documents . . . 407
Analyzing and Fixing Library and Document Information . . . 408

45 Replicating Database Information 411

Replicating Users, Resources, and Groups . . . 411
Replicating Secondary Domains, Post Offices, and Libraries . . . 412
Synchronizing the Primary Domain from a Secondary Domain . . . 412

46 Managing Database Disk Space 413

Gathering Mailbox Statistics . . . 413
Reducing the Size of User and Message Databases . . . 414
Reclaiming Disk Space in Domain and Post Office Databases . . . 416
Reducing the Size of Libraries and Document Storage Areas . . . 416
    Archiving and Deleting Documents . . . 417
    Deleting Activity Logs . . . 418

47 Troubleshooting Database Problems 419

48 Backing Up GroupWise Databases 421

Backing Up a Domain . . . 421
Backing Up a Post Office . . . 421
Backing Up a Library and Its Documents . . . 422
Backing Up Individual Databases . . . 422

49 Restoring GroupWise Databases from Backup 423

Restoring a Domain . . . 423
Restoring a Post Office . . . 423
Restoring a Library . . . 424
Restoring an Individual Database . . . 425
Restoring Deleted Mailbox Items . . . 425
    Setting Up a Restore Area . . . 425

Restoring a User's Mailbox Items 427
Letting Client Users Restore Their Own Mailbox Items 427
Recovering Deleted GroupWise Accounts 428

50 Retaining User Messages 429

How Message Retention Works 429
What GroupWise Does 429
What the Message Retention Application Does 430
Acquiring a Message Retention Application 430
Enabling Message Retention 431

51 Stand-Alone Database Maintenance Programs 433

GroupWise Check 433
GWCheck Functionality 433
Using GWCheck on Linux 435
Using GWCheck on Windows 435
Performing Mailbox/Library Maintenance Using GWCheck 436
Executing GWCheck from a Linux Script 438
Executing GWCheck from a Windows Batch File 438
GWCheck Startup Switches 438
GroupWise Database Copy Utility 441
DBCopy Functionality 441
Using DBCopy on Linux 441
Using DBCopy on Windows 442
Using DBCopy Startup Switches 443
GroupWise Backup Time Stamp Utility 444
GWTMSTMP Functionality 444
Running GWTMSTMP on Linux 445
Running GWTMSTMP on Windows 446
GWTMSTMP Startup Switches 446

Part IX Users 451

52 Creating GroupWise Accounts 453

Establishing a Default Password for All New GroupWise Accounts 453
Creating GroupWise Accounts by Importing Users from an LDAP Directory 453
Manually Creating GroupWise Accounts 454
Configuring New GroupWise Accounts 455
Adding User Photos to the System Address Book 456
Educating Your New Users 456
GroupWise Client 457
GroupWise WebAccess 457
GroupWise WebAccess Mobile 457

53 Managing GroupWise Accounts and Users 459

Adding a User to a Group 459
Allowing Users to Modify Groups 459
Adding a Global Signature to Users' Messages 460
Creating Global Signatures 460
Setting a Default Global Signature 460
Assigning Global Signatures to GWIAs 461
Assigning Global Signatures to GroupWise Client Users. 461

Excluding Global Signatures . . . 461
Moving GroupWise Accounts . . . 462
Live Move vs. File Transfer Move . . . 462
Preparing for a User Move . . . 462
Moving a GroupWise Account to Another Post Office . . . 463
Monitoring User Move Status . . . 464
Renaming Users and Their GroupWise Accounts . . . 466
Changing the LDAP Directory Association of Users . . . 466
Associating GroupWise Users with an LDAP Directory . . . 467
Migrating From eDirectory to Active Directory . . . 467
Dissociating GroupWise Users from an LDAP Directory . . . 470
Managing Mailbox Passwords . . . 470
Creating or Changing a Mailbox Password . . . 470
Removing a Mailbox Password . . . 471
Managing User Email Addresses . . . 471
Ensuring Unique Email Addresses . . . 471
Publishing Email Addresses to Your LDAP Directory . . . 471
Changing a User's Internet Addressing Settings . . . 472
Changing a User's Visibility in the Address Book . . . 472
Synchronizing User Information . . . 472
Disabling and Enabling GroupWise Accounts . . . 473
Unlocking GroupWise Accounts . . . 473
Checking GroupWise Account Usage . . . 473
Forcing Inactive Status . . . 474
Removing GroupWise Accounts . . . 474
Deleting a GroupWise Account . . . 474
Expiring a GroupWise Account . . . 475
Managing Expired or Expiring GroupWise Accounts . . . 475

54 Configuring Single Sign-On 477

Configuring Single Sign-On with KeyShield . . . 477
System Requirements . . . 477
Configuring KeyShield SSO . . . 477
Configuring Single Sign-On with Active Directory . . . 478
Windows POA . . . 478
Linux POA . . . 478
Enabling eDirectory and CASA Single Sign-on . . . 479

Part X Groups 481

55 Understanding Groups 483

Personal Groups . . . 483
GroupWise Groups . . . 483
LDAP Groups . . . 483

56 Creating and Managing Groups 485

Creating a New Group . . . 485
Adding Members to a Group . . . 485
Configuring a New Group . . . 486
Removing Members from a Group . . . 487
Moving a Group . . . 487
Renaming a Group . . . 487
Controlling Access to a Group . . . 488

Enabling Users to Modify a Group 488
Selecting the Users Who Can Modify a Group 488
Granting Group Modification Rights to a User 488
Deleting a Group. 489
Managing Email Addresses 489
Changing a Group's Internet Addressing Settings 489
Changing a Group's Visibility in the Address Book 490
Adding External Users to a Group 490

Part XI Resources 491

57 Creating Resources 493

Understanding Resources 493
Resource Objects. 493
Resource Types 493
Resource Mailboxes. 493
Resource Owners 494
Planning Resources 494
Creating a New Resource. 494
Configuring the New Resource 495

58 Managing Resources 497

Creating Rules for a Resource 497
Creating an Auto-Accept Rule 497
Creating an Auto-Decline Rule. 498
Changing a Resource's Owner 498
Adding a Resource to a GroupWise Group 499
Moving a Resource. 499
Renaming a Resource 500
Deleting a Resource 500
Managing Resource Email Addresses 500
Changing a Resource's Internet Addressing Settings 500
Changing a Resource's Visibility in the Address Book. 500

Part XII Nicknames 501

59 Understanding Nicknames 503

60 Manually Creating Nicknames 505

Manually Creating a Nickname for a User 505
Manually Creating a Nickname for a Resource. 505
Manually Creating a Nickname for a Group 506

61 Configuring Automatic Nickname Creation 507

62 Managing Nicknames 509

Part XIII Libraries and Documents 511

63 Document Management Services Overview 513

Libraries . . . 513
Document Storage Areas . . . 513
Documents . . . 514

64 Creating and Managing Libraries 515

Planning a Library . . . 515
  Selecting the Post Office That the Library Will Belong To . . . 515
  Choosing the Library Name . . . 515
  Deciding Where to Store Documents . . . 516
  Setting the Start Version Number . . . 516
  Figuring Maximum Archive Size . . . 517
Creating a Library . . . 517
Seeing the New Library in the GroupWise Client . . . 518
Managing Libraries . . . 518
  Managing Library Access . . . 518
  Adding and Training Librarians . . . 520
  Maintaining Library Databases . . . 523
  Deleting a Library . . . 523
Library Worksheet . . . 523

65 Managing Document Storage Areas in Libraries 525

Adding a Document Storage Area . . . 525
Deleting a Document Storage Area . . . 526

66 Creating and Managing Documents 527

Adding Documents to Libraries . . . 527
  Creating New Documents in the GroupWise Client . . . 527
  Importing Existing Documents into the GroupWise DMS System . . . 527
  Managing Groups of Documents . . . 527
Indexing Documents in Libraries . . . 528
  Understanding DMS Indexing . . . 528
Managing Documents in Libraries . . . 529
  Archiving and Deleting Documents . . . 529
  Backing Up and Restoring Archived Documents . . . 530
  Handling Orphaned Documents . . . 531

Part XIV Client 533

67 Using GroupWise Client Custom Installation Options 535

Using GWTuner . . . 535
Extracting the GroupWise Software . . . 536

68 Setting Up GroupWise Client Modes and Accounts 539
GroupWise Client Modes . . . 539
Online Mode . . . 539
Caching Mode . . . 539
Remote Mode . . . 541
Email Accounts . . . 544
Accounts Menu . . . 544
Enabling POP3, IMAP4, and NNTP Account Access in Online Mode . . . 544

69 Setting Defaults for the GroupWise Client Options 545
Client Options Summary . . . 545
Setting Client Options . . . 550
Modifying Environment Options . . . 551
Modifying Send Options . . . 563
Modifying Calendar Options . . . 573
Modifying Security Options . . . 577
Modifying Integrations Options . . . 579
Modifying Documents Options . . . 581
Resetting Client Options to Default Settings . . . 581

70 Distributing the GroupWise Client 583
Using Client Auto-Update to Distribute the GroupWise Client Software . . . 583
Using the POA to Distribution the GroupWise Client Software . . . 583
Using Your Web Server to Distribute the GroupWise Client Software . . . 584
Working with the Setup.cfg File . . . 587
Understanding the User’s Client Auto-Update Experience . . . 592
Using ZENworks Configuration Management to Distribute the GroupWise Client . . . 592

71 Supporting the GroupWise Client in Multiple Languages 593

72 Tools for Analyzing and Correcting GroupWise Client Problems 595
GroupWise Exception Handler for the GroupWise Client . . . 595
GroupWise Check . . . 595

73 Startup Options for the GroupWise Client 597

Part XV WebAccess 599

74 Accessing Your GroupWise Mailbox in a Web-Based Environment 601
Using WebAccess on a Desktop Workstation . . . 601
Using WebAccess on a Tablet . . . 601
Using the WebAccess Basic Interface on a Mobile Device . . . 602

75 Scaling Your GroupWise WebAccess Installation 603
WebAccess Configurations . . . 603
Basic WebAccess Application Installation . . . 603
Multiple POAs for a WebAccess Application . . . 603
Multiple DVAs for a WebAccess Application . . . 604
Multiple WebAccess Applications and Web Servers for a Large WebAccess Installation . . . 604
WebAccess Installation on Additional Web Servers . . . 605

76 Configuring the WebAccess Application 607

Customizing the WebAccess Application . . . 607
- Editing the webacc.cfg File . . . 608
- Configuring the WebAccess Application with Multiple POAs for Fault Tolerance . . . 608
- Configuring WebAccess Application with Multiple DVAs for Attachment Viewing . . . 609
- Disabling Caching of Attachments . . . 609
- Adjusting Session Security . . . 610
- Accommodating Single Sign-On Products . . . 610
- Putting WebAccess Configuration Changes into Effect . . . 610

Managing User Access . . . 611
- Setting the Timeout Interval for Inactive WebAccess Sessions . . . 611
- Customizing Auto-Save Functionality . . . 612
- Preventing Users from Changing Their GroupWise Passwords in WebAccess . . . 613
- Helping Users Who Forget Their GroupWise Passwords . . . 613
- Controlling WebAccess Usage . . . 613

Customizing User Functionality . . . 615
- Customizing the WebAccess User Interface with Your Company Logo . . . 615
- Controlling the WebAccess New Item Notification Sound . . . 615
- Customizing Auto-Refresh Functionality . . . 616
- Controlling Viewable Attachment Types . . . 617
- Controlling Viewable Attachment Size . . . 617
- Customizing the Default Calendar View . . . 618
- Customizing the Default List Functionality . . . 618
- Customizing New Item Handling for Tablet Users . . . 618
- Enabling an LDAP Address Book . . . 619

77 Monitoring the WebAccess Application 621

Using the WebAccess Application Console . . . 621
- Enabling the WebAccess Application Console . . . 621
- Using the WebAccess Application Console . . . 621

Using WebAccess Application Log Files . . . 621
- Locating WebAccess Application Log Files . . . 621
- Configuring WebAccess Application Log Settings . . . 622
- Viewing WebAccess Application Log Files . . . 622
- Interpreting WebAccess Application Log File Information . . . 622

Part XVI Calendar Publishing Host 623

78 Configuring the Calendar Publishing Host 625

Using the CalPub Admin Console . . . 625
- Logging In to the CalPub Admin Console . . . 625
- Changing Post Office Settings . . . 625
- Adjusting Log Settings . . . 626
- Configuring Authentication . . . 626
- Customizing the Calendar Publishing Host Logo . . . 627
- Putting the CalPub Host Configuration Changes into Effect . . . 627

Using the calhost.cfg File . . . 627
- Editing the calhost.cfg File . . . 627
- Setting the Published Calendar Auto-Refresh Interval . . . 628
- Setting the Default Published Calendar View . . . 628
- Controlling Items Displayed . . . 628
- Configuring an External POA IP Address . . . 629
- Providing an SSL Trusted Root Certificate . . . 629

79 Monitoring Calendar Publishing 631

Viewing Calendar Publishing Status in the POA Console . . . 631
Using Calendar Publishing Host Log Files . . . 631
Using POA Log Files . . . 631

80 Creating a Corporate Calendar Browse List 633

81 Managing Your Calendar Publishing Host 635

Adding Multiple Calendar Publishing Hosts . . . 635
Assigning a Different Calendar Publishing Host to Users . . . 635
Editing Calendar Publishing Host Configuration . . . 636
Deleting a Calendar Publishing Host . . . 636

Part XVII Monitor 637

82 Understanding the Monitor Agent Consoles 639

Windows Monitor Agent Server Console . . . 639
Monitor Agent Console . . . 639
Monitor Web Console . . . 639

83 Configuring the Monitor Agent 641

Selecting Agents to Monitor . . . 641
- Filtering the Agent List . . . 641
- Adding an Individual Agent . . . 642
- Adding All Agents on a Server . . . 642
- Adding All Agents on a Subnet . . . 642
- Removing Added Agents . . . 642

Creating and Managing Agent Groups . . . 643
- Creating an Agent Group . . . 643
- Managing Agent Groups . . . 643
- Configuring an Agent Group . . . 643

Configuring Monitoring Protocols . . . 644
- Configuring the Monitor Agent for HTTP . . . 644
- Configuring the Monitor Agent for SNMP . . . 644

Configuring Polling of Monitored Agents . . . 645
Configuring Email Notification for Agent Problems . . . 645
- Configuring Email Notification . . . 645
- Customizing Notification Thresholds . . . 646

Configuring SNMP Trap Notification for Agent Problems . . . 647
Securing the Monitor Web Console . . . 647
Configuring Monitor Agent Log Settings . . . 647
Configuring Proxy Service Support for the Monitor Console . . . 648
Supporting the GroupWise High Availability Service on Linux . . . 649

84 Configuring the Monitor Application 651

Editing the gwmonitor.cfg File . . . 651
Setting the Timeout Interval for Inactive Sessions . . . 651
Adjusting Session Security . . . 652
Accommodating Single Sign-On Products . . . 652
Configuring Monitor Application Log Settings . . . 652

Locating Monitor Application Log Files. 653
Configuring Monitor Application Log Settings 653
Viewing Monitor Application Log Files 653
Putting the Monitor Configuration Changes into Effect 654
Accepting the Default Time Interval 654
Changing the Default Time Interval 654
Immediately Putting the Configuration Changes into Effect 654

85 Using GroupWise Monitor 655

Using the Monitor Agent Console 655
Viewing All Agents 655
Viewing Problem Agents 655
Viewing an Agent Console 655
Polling the Agents for Updated Status Information 656
Using the Monitor Web Console 656
Generating Reports. 657
Link Trace Report. 657
Link Configuration Report 657
Image Map Report 658
Environment Report 662
User Traffic Report 662
Link Traffic Report 663
Message Tracking Report 663
Performance Testing Report. 664
Connected User Report 664
Gateway Accounting Report. 664
Trends Report 664
Down Time Report 664
Measuring Agent Performance 665
Setting Up an External Monitor Domain for Agent Performance 665
Configuring the Link for the External Monitor Domain 665
Configuring the Monitor Agent for Agent Performance Testing 666
Viewing Agent Performance Data 666
Viewing an Agent Performance Report 666
Receiving Notification of Agent Performance Problems. 667
Collecting Gateway Accounting Data 667
Setting Up an External Monitor Domain for Gateway Accounting 667
Configuring the Link for the External Monitor Domain 668
Configuring the Monitor Agent to Communicate through the External Monitor Domain. 668
Setting Up an External Post Office and External User for the Monitor Agent. 668
Receiving and Forwarding the Accounting Files 669
Viewing the Gateway Accounting Report 670
Assigning Responsibility for Specific Agents 670
Searching for Agents. 671

86 Comparing the Monitor Consoles 673

87 Using Monitor Agent Startup Switches 675

--hapassword 676
--hapoll 676
--hauser. 677
--help. 677
--home. 677
--httpagentpassword 678
--httpagentuser 678

--httpcertfile . . . 678
--httpmonpassword . . . 679
--httpmonuser . . . 679
--httpport . . . 679
--httpssl . . . 679
--ipa . . . 680
--ipp . . . 680
--lang . . . 680
--log . . . 681
--monwork . . . 681
--nosnmp . . . 682
--pollthreads . . . 682
--proxy . . . 682
--tcpwaitconnect . . . 682

Part XVIII Security Administration 683

88 Native GroupWise Security 685

89 GroupWise Passwords 687

Mailbox Passwords . . . 687
- Using Post Office Security Instead of GroupWise Passwords . . . 687
- Requiring GroupWise Passwords . . . 688
- Managing GroupWise Passwords . . . 688
- Using LDAP Passwords Instead of GroupWise Passwords . . . 690
- Bypassing GroupWise Passwords with Single Sign-On . . . 690
- Bypassing GroupWise Passwords to Respond to Corporate Mandates . . . 691

Agent Passwords . . . 691
- Facilitating Access to Remote Servers . . . 691
- Protecting the Agent Consoles . . . 691
- Protecting the GroupWise Monitor Console . . . 692

90 Encryption and Certificates 693

Personal Digital Certificates, Digital Signatures, and S/MIME Encryption . . . 693
Server Certificates and SSL Encryption . . . 695
- Using a Self-Signed Certificate from the GroupWise Certificate Authority . . . 695
- Using a Commercially Signed Certificate . . . 695
- Configuring the Agents to Use SSL . . . 697

Trusted Root Certificates and LDAP Authentication . . . 698

91 LDAP Directories 699

Accessing Public LDAP Directories from GroupWise . . . 699
Authenticating to GroupWise with Passwords Stored in an LDAP Directory . . . 699
- Access Method . . . 699
- LDAP User Name and Password . . . 700

Accessing S/MIME Certificates in an LDAP Directory . . . 700

92 Message Security 701

93 GroupWise Address Book Security 703

LDAP Directory Information Displayed in the GroupWise Address Book 703
Suppressing the Contents of the User Description Field 703
Controlling GroupWise Object Visibility in the GroupWise Address Book. 704
Controlling GroupWise Object Visibility between GroupWise Systems 704

94 Spam Protection 705

Configuring the GWIA for Spam Protection 705
Configuring the GroupWise Client for Spam Protection 705

95 Virus Protection 707

Part XIX Security Policies 709

96 Securing GroupWise Data 711

Limiting Physical Access to GroupWise Servers. 711
Securing File System Access 711
Securing Domains and Post Offices 711

97 Securing GroupWise Agents 713

Setting Up SSL Connections. 713
Protecting Agent Consoles 713
Protecting Agent Startup Files 713
Protecting Agent and Application Log Files. 714
Preventing the GWIA from Acting as a Relay Host 714
Protecting Agent Processes on Linux 714
Protecting Trusted Applications. 714

98 Securing GroupWise System Access 717

Using a Proxy Server with Client/Server Access. 717
Using LDAP Authentication for GroupWise Users 717
Managing Mailbox Passwords 717
Enabling Intruder Detection 717

99 Secure Migrations 719

GroupWise Server Migration Utility 719
Source Server Credentials 719
Destination Server root Password 719
Agent Startup Files. 719

Part XX Appendixes 721

A GroupWise Port Numbers 723

Opening Ports for GroupWise Agents and Applications 723

Opening Ports on OES Linux . . . 723
Opening Ports on SLES . . . 724
Opening Ports on Windows . . . 725
Protocol Flow Diagram with Port Numbers . . . 726
Post Office Agent Port Numbers . . . 727
Message Transfer Agent Port Numbers . . . 728
Internet Agent Port Numbers . . . 728
Document Viewer Agent Port Numbers . . . 729
WebAccess Application Port Numbers . . . 729
Calendar Publishing Host Port Numbers . . . 730
Monitor Agent Port Number . . . 730
Monitor Application Port Numbers . . . 730
GroupWise High Availability Service Port Number (Linux Only) . . . 731
Port Numbers for Products Frequently Used with GroupWise . . . 731
GroupWise Messenger Port Number . . . 731
GroupWise Mobility Service Port Numbers . . . 732
BlackBerry Enterprise Server for Micro Focus GroupWise Port Number . . . 732

B GroupWise URLs 733

C Linux Basics for GroupWise Administration 735

Linux Operating System Commands . . . 735
Basic Commands . . . 735
File and Directory Commands . . . 736
Process Commands . . . 737
Disk Usage Commands . . . 737
Package Commands . . . 737
File System Commands . . . 738
Network Commands . . . 738
Linux Core File . . . 738
GroupWise Directories and Files on Linux . . . 738
Linux Agent Software Subdirectories . . . 739
Linux Agent Startup and Configuration Files . . . 739
GroupWise Commands on Linux . . . 740

About This Guide

This Micro Focus *GroupWise 18 Administration Guide* helps you maintain all components of your GroupWise system.

The following resources provide additional information about using GroupWise 18:

- Micro Focus Support and Knowledgebase (http://www.novell.com/support/)

  To search the GroupWise documentation from the Micro Focus Support website, click **Advanced Search**, select **Documentation** in the **Search In** drop-down list, select **GroupWise** in the **Products** drop-down list, type the search string, then click **Search**.
- GroupWise Support Forums (https://forums.novell.com/forumdisplay.php/356-GroupWise)
- GroupWise Support Community (http://www.novell.com/support/kb/product.php?id=GroupWise)
- GroupWise Cool Solutions (https://www.novell.com/communities/coolsolutions/category/groupwise/)

Audience

This guide is intended for those who administer a GroupWise system on Linux or Windows. Some background knowledge of the host operating system is assumed.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation.

Additional Documentation

For additional GroupWise documentation, see the following guides at the GroupWise 18 documentation website (http://www.novell.com/documentation/groupwise18):

- *Installation Guide*
- *Server Migration Guide*
- *Administration Guide*
- *Multi-System Administration Guide*
- *Interoperability Guide*
- *Troubleshooting Guides*
- *GroupWise User Frequently Asked Questions (FAQ)*
- *GroupWise User Guides*
- *GroupWise User Quick Starts*

System

- Chapter 1, “GroupWise System Administration,” on page 33
- Chapter 2, “GroupWise Administration Console,” on page 35
- Chapter 3, “GroupWise Administrators,” on page 45
- Chapter 4, “GroupWise System Tools,” on page 49
- Chapter 5, “GroupWise Address Book,” on page 69
- Chapter 6, “LDAP Directories and Servers in Your GroupWise System,” on page 79
- Chapter 7, “Multilingual GroupWise Systems,” on page 85

1 GroupWise System Administration

As a GroupWise system administrator, it is your responsibility to keep your GroupWise system running smoothly for your GroupWise users. This *GroupWise 18 Administration Guide* provides a wealth of information to help you accomplish this task. This System section provides an overview of the GroupWise Administration console and its capabilities. It summarizes administrative tasks that affect your GroupWise system as a whole and provides links to more specialized instructions.

The following sections of the *Administration Guide* detail the GroupWise objects where GroupWise information is stored. Instructions are provided for creating and managing all GroupWise object types.

- "Domains" on page 91
- "Post Offices" on page 117
- "Users" on page 451
- "Resources" on page 491
- "Groups" on page 481

The following sections of the *Administration Guide* detail the GroupWise software components that make your GroupWise system run. Instructions are provided for configuring, monitoring, and optimizing each software component.

- "Post Office Agent" on page 133
- "Message Transfer Agent" on page 221
- "Internet Agent" on page 263
- "Document Viewer Agent" on page 359
- "WebAccess" on page 599
- "Calendar Publishing Host" on page 623
- "Monitor" on page 637

The following additional sections of the *Administration Guide* provide supporting details and background information:

- "Databases" on page 389
- "Nicknames" on page 501
- "Libraries and Documents" on page 511
- "Client" on page 533
- "Security Administration" on page 683
- "Security Policies" on page 709

2 GroupWise Administration Console

The GroupWise Administration console is a web-based administration tool that provides convenient access to your GroupWise system in your web browser. Your web browser can connect to the GroupWise Administration Service on any domain server. From any domain server, you can access other domain servers and post office servers throughout your GroupWise system.

Accessing the GroupWise Admin Console

1 Click the Admin console icon on your desktop.

   or

   Display the following URL in your web browser:

   `https://groupwise_server_address:admin_port/gwadmin-console`

   Replace *groupwise_server_address* with the IP address or DNS hostname of the GroupWise server. If you are not using the default Admin port, replace *admin_port* with the Admin port number. If you are using the default Admin port number, you do not need to specify it.

2 (Conditional) If you need an introduction to the Admin console, see "Working with the GroupWise Administration Console" in the *GroupWise 18 Installation Guide*.

Connecting to a Domain

Understanding the Need for Domain Connections

You can access the GroupWise Admin console on any server where a domain is located. You should access the Admin console on the primary domain server to perform the following types of administrative tasks:

- Creating and deleting secondary domains
- Performing maintenance on the primary domain database (`wpdomain.db`)
- Creating and deleting post offices in the primary domain, if any

You can access the Admin console on a secondary domain server to perform the following types of administrative tasks:

- Creating and deleting post offices in that domain
- Performing maintenance on the secondary domain database (`wpdomain.db`)
- Performing maintenance on post office databases (`wphost.db`)
- Performing maintenance on user/resource databases (`userxxx.db`) in post offices
- Performing maintenance on message databases (`msgnnn.db`) in post offices

In order to access a domain, the GroupWise Admin Service must be running on the domain server.

Selecting a Domain

1 In the GroupWise Admin console, select the domain in the **Connected Domain** drop-down list.

  If the Admin Service on the target domain server is down, a message notifies you, and you cannot connect to the domain.

Getting Acquainted with the GroupWise Admin Console

If you did not get acquainted with the GroupWise Admin console by creating or upgrading your GroupWise system, see the following sections of the *GroupWise 18 Installation Guide*:

- "Making the Most of the System Overview"
- "Finding Objects in Object Lists"
- "Finding Frequently Used Objects Quickly"
- "Working with Objects and Object Properties"
- "Using System Tools"

Monitoring Background Administrative Tasks

You can immediately perform most administrative tasks in the GroupWise Admin console. However, some administrative tasks can be time consuming. Therefore, the Admin console runs the tasks as background processes so that you can continue with other work in the Admin console. Background tasks include:

- Database maintenance
- User import

The number of background tasks that the Admin console is running displays in the upper right corner of the Admin console window.

1 Click the number of tasks to display the Background Tasks list.

  Tasks remain on the list until you clear them.

2 Click the name of a task to display details about it.

3 Click **Refresh** to display the current status of all tasks that are still in progress.

4 Select a task, then click **Cancel/Clear** to stop the task before completion.

Managing the GroupWise Admin Service

The GroupWise Admin Service interacts with your web browser to provide the GroupWise Admin console. For background information about the GroupWise Admin Service, see "Administration Service Architecture" in the *GroupWise 18 Installation Guide*.

- "Linux: Managing the GroupWise Admin Service" on page 37
- "Windows: Managing the GroupWise Admin Service" on page 38

Linux: Managing the GroupWise Admin Service

There are a variety of ways to start and stop the GroupWise Admin Service on the command line. Information about Admin Service functioning is found in the Admin Service log file.

- "Using the rcgrpwise Command" on page 37
- "Using the gwadminutil Command" on page 37
- "Using the gwsc Command" on page 37
- "Using the GroupWise Admin Service Log File" on page 37

Using the rcgrpwise Command

Use the following `rcgrpwise` commands to start and stop the GroupWise Admin Service:

```
rcgrpwise start gwadminservice
rcgrpwise restart gwadminservice
rcgrpwise stop gwadminservice
```

When you use the following `rcgrpwise` commands, the GroupWise Admin Service starts and stops along with the GroupWise agents on the server:

```
rcgrpwise start
rcgrpwise restartall
rcgrpwise stop
```

Using `rcgrpwise restart` restarts the GroupWise agents, but not the GroupWise Admin Service

Using the gwadminutil Command

Use the following `gwadminutil` commands to start and stop the GroupWise Admin Service:

```
gwadminutil services -start gwadminservice
gwadminutil services -stop gwadminservice
```

Using the gwsc Command

Use the following `gwsc` commands as shortcuts for the `gwadminutil` commands to start and stop and GroupWise Admin Service:

```
gwsc -start gwadminservice
gwsc -stop gwadminservice
```

Using the GroupWise Admin Service Log File

In general, the GroupWise Admin Service runs smoothly. If something unusual happens, you can check the GroupWise Admin Service log file for more information. The GroupWise Admin Service log file is located in the following folder:

```
/var/log/novell/groupwise/gwadmin
```

Windows: Managing the GroupWise Admin Service

There are a variety of ways to start and stop the GroupWise Admin Service on the command line. Information about Admin Service functioning is found in the Admin Service log file.

- "Using the Windows Services Administrative Tool" on page 38
- "Using the gwadminutil Command on the Windows Command Line" on page 38
- "Using the gwsc Command on the Windows Command Line" on page 38
- "Using the GroupWise Admin Service Log File" on page 38

Using the Windows Services Administrative Tool

The GroupWise Admin Service can be managed just like any other Windows service.

1. On the Windows Control Panel, click **Administrative Tools > Services**.
2. Scroll down the **GroupWise Administration Service**.
3. Right-click **GroupWise Administration Service**, then click an administrative task.

Using the gwadminutil Command on the Windows Command Line

Use the following `gwadminutil` commands to start and stop the GroupWise Admin Service:

```
gwadminutil services -start gwadminservice
gwadminutil services -stop gwadminservice
```

Using the gwsc Command on the Windows Command Line

Use the following `gwsc` commands as shortcuts for the `gwadminutil` commands to start and stop and GroupWise Admin Service:

```
gwsc -start gwadminservice
gwsc -stop gwadminservice
```

Using the GroupWise Admin Service Log File

In general, the GroupWise Admin Service runs smoothly. If something unusual happens, you can check the GroupWise Admin Service log file for more information. The GroupWise Admin Service log file is located in the following folder:

```
c:\ProgramData\Micro Focus\GroupWise\gwadmin
```

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

Using the GroupWise Administration Utility

The GroupWise Administration Utility (GWAdminUtil) enables you to perform security management, agent service management, and database management tasks on the command line. The *GroupWise 18 Utilities Reference* provides details.

- "GroupWise Administration Utility"
  - gwadminutil
  - gwsc
- "GroupWise Administration Utility — Security Options"
  - Resetting the GroupWise Super Admin User Name and Password
  - Changing the Authentication Mode for the GroupWise Installation Console
  - Managing SSL Certificates with the GroupWise Certificate Authority
  - Installing a New SSL Certificate on a Domain or Post Office Server
- "GroupWise Administration Utility — Service Options"
  - Managing the GroupWise Agent Services on the Command Line
  - Configuring the GroupWise Admin Service for Clustering
- "GroupWise Administration Utility — Database Options"
  - Validating a Domain or Post Office Database
  - Recovering a Domain or Post Office Database
  - Rebuilding a Domain or Post Office Database
  - Reindexing a Domain or Post Office Database
  - Reclaiming Unused Space in a Database
  - Synchronizing the Primary Domain with a Secondary Domain
  - Converting a Secondary Domain into the Primary Domain
  - Releasing a Domain from Your GroupWise System
  - Merging a Domain into Your GroupWise System
- "GroupWise Database Utilities"
  - GroupWise Check (GWCheck)
  - GroupWise Database Copy (DBCopy)
  - GroupWise Database Backup Time Stamp (GWTMSTMP)

All activities performed by using the GroupWise Administration Utility are logged in the `gwadminutil.log` file in the following folder:

Linux:	`/var/log/novell/groupwise/gwadmin`
Windows:	`c:\ProgramData\Micro Focus\GroupWise\gwadmin`

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

Using an LDAP Directory Management Tool for Adding LDAP Users and Groups to GroupWise

In an environment where GroupWise users are associated with User objects in an LDAP directory, it can be convenient to assign new GroupWise users to post offices at the same time as they are created in the LDAP directory. It can also be convenient to use LDAP groups as GroupWise groups.

GroupWise integration is available for both Micro Focus iManager and Microsoft Management Console (MMC).

Adding GroupWise Users and Groups in Micro Focus iManager

If your organization has one administrator for GroupWise and a different administrator for eDirectory, you can install the GroupWise plugin for iManager for the eDirectory administrator in order to streamline the process of adding users on your network. The eDirectory administrator can add new users in iManager, and then immediately add the new users to GroupWise post offices.

- "Installing the GroupWise Plugin for iManager" on page 40
- "Configuring the GroupWise Plugin for iManager" on page 40
- "Adding GroupWise Users in iManager" on page 41
- "Adding an eDirectory Group to GroupWise in iManager" on page 41

Installing the GroupWise Plugin for iManager

1. In the GroupWise Admin console, add eDirectory as an LDAP directory.

   For instructions, see "Setting Up an LDAP Directory" on page 79.
2. In the GroupWise Admin console, configure LDAP user synchronization between GroupWise and eDirectory.

   For instructions, see "Configuring User Synchronization for an LDAP Directory" on page 80.
3. Log in to iManager, then click **Configure** on the menu bar.
4. Click **Plug-in Installation > Available Micro Focus Plug-In Modules**.
5. In the list of plugins, select **GroupWise Plugins**, then click **Install**.
6. When the installation is complete, click **Close**.
7. Restart Tomcat to make the GroupWise plugin available in iManager.
8. Continue with Configuring the GroupWise Plugin for iManager.

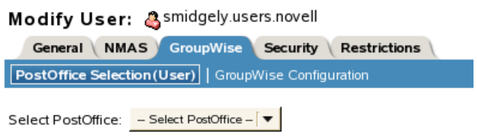
TIP: If you need to manually download and install the GroupWise iManager plugin, visit https://download.novell.com in your web browser, then select **iManager** and your version number from the P**roduct or Technology** drop-down menu. Click **Submit**, and the GroupWise plugin for iManager appears below the search area. Follow the instructions in the download to install the plugin.

Configuring the GroupWise Plugin for iManager

1. Log in to iManager again.
2. Click **Roles and Tasks** on the menu bar, then click **Directory Administration > Modify Object** on the navigation bar.

3 On the Modify Object page, browse to and select the eDirectory administrator user, then display the Object properties.

A **GroupWise** tab is now available.



4 Click the **GroupWise** tab, then click **GroupWise Configuration**.

5 Provide the configuration information about your GroupWise system:

5a Specify the IP address of the primary domain server and the port number for the Admin Service (9710 by default).

5b Specify the GroupWise Directory Name that represents eDirectory in your GroupWise system.

You set up this Directory name in Step 1 in "Installing the GroupWise Plugin for iManager" on page 40.

5c Specify the GroupWise Super Admin user name and password.

5d Click **OK**.

6 Continue with Adding GroupWise Users in iManager.

Adding GroupWise Users in iManager

1 In iManager, create a new eDirectory user as usual., then click **Modify**.

2 Click the **GroupWise** tab.

3 Select the new user's post office, then click **OK**.

The new user is quickly available in the GroupWise Admin console. GroupWise establishes the user's email address.

If the eDirectory administrator changes the user's name in eDirectory, the changes synchronize over to GroupWise.

If you want the user's email address to synchronize over to eDirectory, see "Configuring User Synchronization for an LDAP Directory" on page 80.

4 Continue with Adding an eDirectory Group to GroupWise in iManager.

Adding an eDirectory Group to GroupWise in iManager

You can use an eDirectory group as a GroupWise group by associating it with a GroupWise post office.

1 In iManager, create a new group as usual, then click **Modify**.

NOTE: You cannot associate an existing eDirectory group with GroupWise.

---

2 Click the **GroupWise** tab.

3 Select the post office that you want to own the new group, then click **OK**.

The new group quickly displays in the GroupWise Admin console, but you cannot add members to the group in the Admin console.

4 In iManager, add GroupWise users as members of the group.

5 In the GroupWise Admin console, browse to and click the name of the new group, then click **Synchronize** to immediately pull the group membership from eDirectory into GroupWise.

NOTE: On an ongoing basis, LDAP user synchronization transfers changes in the group membership from eDirectory over to GroupWise. For more information, see "Configuring User Synchronization for an LDAP Directory" on page 80. You cannot change group membership in the GroupWise Admin console.

GroupWise establishes the new group's email address.

If you want the group's email address to synchronize over to eDirectory, see "Publishing Email Addresses to Your LDAP Directory" on page 471.

NOTE: After you associate an eDirectory group with a GroupWise post office, the **GroupWise** tab no longer appears in iManager. You can see which post office the group is associated with by displaying the Group object properties in the GroupWise Admin console.

Managing GroupWise Users and Groups in Microsoft Management Console

If your organization has one administrator for GroupWise and a different administrator for Active Directory, you can install the GroupWise plugin for Microsoft Management Console (MMC) for the Active Directory administrator in order to streamline the process of adding new users on your network. The Active Directory administrator can add the new users in the Computers and Users component of MMC, and then immediately add the new users to GroupWise post offices.

- "Installing the GroupWise Plugin for Microsoft Management Console" on page 42
- "Adding a GroupWise User in Active Directory" on page 43
- "Adding a GroupWise User to a GroupWise Group in Active Directory" on page 43

Installing the GroupWise Plugin for Microsoft Management Console

1 In the GroupWise Admin console, add Active Directory as an LDAP directory.

For instructions, see "Setting Up an LDAP Directory" on page 79.

2 In the GroupWise Admin console, configure LDAP user synchronization between GroupWise and Active Directory.

For instructions, see "Configuring User Synchronization for an LDAP Directory" on page 80.

3 Download the *GroupWise 18* Windows software image to the Windows server where you want to run Computers and Users to create GroupWise users and groups.

4 Run `setup.exe` at the root of the downloaded *GroupWise 18* software image to start the GroupWise Installation Wizard.

5 Click **GroupWise MMC Plugin**.

6 Select the language for the Installation Wizard, then click **OK**.

7 Click **Next** to continue.

8 Accept the License Agreement, then click **Next**.

9 Click **Next**, then click **Install**.

10 When the installation complete, click **Finish** to display the GroupWise MMC Plugin Configuration dialog box.

11 Configure the MMC Plugin for GroupWise:

11a Specify the IP address of the primary domain server and the port number for the Admin Service (9710 by default).

11b Specify the name of the LDAP Server object that represents Active Directory in your GroupWise system.

You set up this LDAP Server object in Step 1 in "Installing the GroupWise Plugin for Microsoft Management Console" on page 42.

11c Specify the GroupWise Super Admin user name and password.

11d Click **Test** to ensure that you have provided the correct information.

11e Click **OK** to exit the Configuration dialog box, then click **OK** to confirm the successful configuration.

If you need to change the configuration in the future, run the following program:

```
c:\Program Files\Micro Focus\GroupWise MMC Plugin\gwisepluginconfig.exe
```

12 Continue with Adding a GroupWise User in Active Directory.

Adding a GroupWise User in Active Directory

1 In Computers and Users, click **Action > New > User**.

2 In the New Object - User dialog box, provide the standard user information, then click **Next**.

3 Specify and confirm the password, select other password options as needed, then click **Next**.

A new dialog box appears where you can add the user to a post office.

4 Select the new user's post office, then click **Next**.

5 Click **Finish**.

The new user is quickly available in the GroupWise Admin console. GroupWise establishes the user's email address.

If the Active Directory administrator changes the user's name, the changes synchronize over to GroupWise.

If you want the user's email address to synchronize over to Active Directory, see "Publishing Email Addresses to Your LDAP Directory" on page 471.

6 Continue with Adding a GroupWise User to a GroupWise Group in Active Directory.

Adding a GroupWise User to a GroupWise Group in Active Directory

1 In Computers and Users, click **Actions > New > Group**.

2 In the New Object - Group dialog box, provide the standard group information, then click **Next**.

A new dialog box appears where you can add the group to a post office.

3 Select the post office, then click **Next**.

4 Click **Finish**.

5 In MMC, add GroupWise users as members of the group.

6 In the GroupWise Admin console, browse to and click the name of the new group, then click **Synchronize** to immediately pull the group membership from Active Directory into GroupWise.

NOTE: On an ongoing basis, LDAP user synchronization transfers changes in the group membership from Active Directory over to GroupWise. For more information, see "Configuring User Synchronization for an LDAP Directory" on page 80. You cannot change group membership in the GroupWise Admin console.

GroupWise establishes the new group's email address.

If you want the group's email address to synchronize over to eDirectory, see "Publishing Email Addresses to Your LDAP Directory" on page 471.

NOTE: After you associate an Active Directory group with a GroupWise post office, you cannot see the post office that the group belongs to in MMC. You can see this information by displaying the Group object properties in the GroupWise Admin console.

3 GroupWise Administrators

The GroupWise Admin console provides options for creating different levels of GroupWise administrators. Each level of administrator has different rights to the Admin console and the HTTP consoles. The following are the available roles and their rights to the different HTTP consoles:

- **System Administrator:** Configuration rights to all MTA, POA, and GWIA consoles.
- **Domain Administrator:** Configuration rights to all MTA, POA, and GWIA consoles in their domain.
- **Post Office Administrator:** Configuration rights to their POA console.

Regarding the HTTP consoles, consider the following:

- Any HTTP user you create for a console, does not have Write access to the consoles.
- Because the DVA does not own or read any databases, access control rules do not apply to the DVA.

Any changes to the HTTP consoles are logged with the user ID of the administrator appended t the log message. The user ID is only logged when logging is set to Verbose or higher.

Managing the GroupWise Super Admin User

The GroupWise Super Admin user is established when your GroupWise system is created or upgraded to GroupWise 18. The Super Admin user has the necessary rights to make any and all changes throughout your GroupWise system. The Super Admin user has automatic intruder lockout functionality. If an incorrect password is entered 5 times in a 1 minute period, the account is locked for 5 minutes.

If you need to change the user name or password for the GroupWise Super Admin, use the GroupWise Administration Utility (GWAdminUtil). For background on using GWAdminUtil, see "Using the GroupWise Administration Utility" on page 39.

IMPORTANT: If your HTTP user and super admin user have the same username and password, when you login with the HTTP user, you have full rights. If the users have different password, the HTTP user with only have read rights to the console. To avoid any complications, please use a different username and password for the super admin user and the HTTP console users.

Use the following command to change the user name for the Super Admin user:

Syntax:

```
gwadminutil setadmin -d /path_to_domain -a new_admin_user_name -p
```

Example:

```
gwadminutil setadmin -d /gwsystem/provo1 -a supergw -p [new_password]
```

When you change the user name of the Super Admin user, you can also specify a new password. If you do not specify the new password on the command line, you are prompted for it.

Use the following command to change the password for the Super Admin user:

Syntax:

```
gwadminutil setadmin -d /path_to_domain -a existing_admin_user_name -p
```

Example:

```
gwadminutil setadmin -d /gwsystem/provo1 -a admin -p [new_password]
```

If you do not specify the new password on the command line, you are prompted for it.

Designating Additional GroupWise System Administrators

As the GroupWise Super Admin, you can give equivalent rights to other GroupWise users. These additional system administrators log in to the GroupWise Admin console using their own personal GroupWise user names and passwords, not the Super Admin user name and password.

Such GroupWise system administrators have rights throughout your GroupWise system, but they cannot create additional system administrators. They can, however, create domain and post office administrator.

1. In the GroupWise Admin console, click **System > Administrators**.
2. Select one or more GroupWise users, then click **OK** to add them to the list of GroupWise system administrators.

Designating Domain Administrators

A domain administrator has administrator rights just for a single domain, and for all post offices and users within that domain. The GroupWise Super Admin or a GroupWise administrator can designate domain administrators.

1. In the GroupWise Admin console, click **System > Administrators**.
2. Select one or more GroupWise users, then click **OK** to add them to the list of domain administrators.

In the GroupWise Admin console, domain administrators cannot perform any administrative tasks that do not pertain to the domain where they have rights. As a result, some parts of the Admin console interface are dimmed when domain administrators log in.

Designating Post Office Administrators

A post office administrator has administrator rights just for a single post office, and for all users within that post office. Any higher level administrator can designate a post office administrator.

1. In the GroupWise Admin console, click **System > Administrators**.
2. Select one or more GroupWise users, then click **OK** to add them to the list of post office administrators.

In the GroupWise Admin console, post office administrators cannot perform any administrative tasks that do not pertain to the post office where they have rights. As a result, some parts of the Admin console interface are dimmed when post office administrators log in.

Designating a Specific User as an Administrator

Any individual GroupWise user can be designated as any level of GroupWise administrator.

1. Browse to and click the name of a user, then click **Objects**.
2. On the **Administrator** tab, click **Add**.
3. Select the type of administrator rights that you want to give to this user.

   If you select **As System Administrator**, that right is added to the user's list of administrator rights.
4. (Conditional) If you select **As Domain Administrator**, select the domain where you want the user to have domain administrator rights, then click **OK**.
5. (Conditional) If you select **As Post Office Administrator**, select the post office where you want the user to have post office administrator rights, then **OK**.

TIP: If you need to remove administrator rights from an individual user, you can do it on the User object, or you can do it in the administrator lists that are provided by using **System > Administrators**.

---

4 GroupWise System Tools

The GroupWise system tools allow you to perform various tasks to configure, maintain, and optimize your GroupWise system. The following sections provide information about the tools listed on the **System** menu in the GroupWise Admin console:

- "Addressing Rules" on page 50
- "Admin-Defined Fields" on page 50
- "Administrators" on page 51
- "Calendar Publishing" on page 51
- "Directory Associations" on page 51
- "Document Viewer Agent" on page 51
- "Email Address Lookup" on page 51
- "Expired Records" on page 51
- "External System Synchronization" on page 51
- "Global Signatures" on page 52
- "Information" on page 52
- "Internet Addressing" on page 52
- "LDAP Directories and Servers" on page 52
- "Licensing" on page 52
- "Legacy" on page 53
- "Link Configuration" on page 54
- "Pending Operations" on page 54
- "Record Enumerations" on page 55
- "Recover Deleted Account" on page 55
- "Restore Area Management" on page 55
- "System Preferences" on page 56
- "Time Zones" on page 61
- "Trusted Applications" on page 64
- "User Import" on page 67
- "User Move Status" on page 67
- "Standalone GroupWise Database Utilities" on page 67

In addition to the system utilities included on the **System** menu in the GroupWise Admin console, GroupWise includes the following standalone utilities:

- GroupWise Check Utility (GWCheck)
- GroupWise Backup Time Stamp Utility (GWTMSTMP)
- GroupWise Database Copy Utility (DBCOPY)

NOTE: If the majority of the items on the *GroupWise System Operations* menu are dimmed, you are connected to a secondary domain in a GroupWise system where *Restrict System Operations to Primary Domain* has been selected under *System Preferences*. This option is selected by default. For more information, see "System Preferences" on page 56.

Addressing Rules

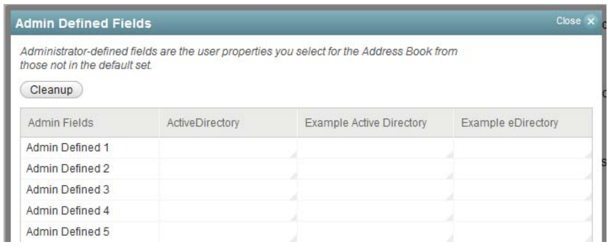
You can use the Addressing Rules tool to configure GroupWise so that users can enter shortened forms of email addresses for use through GroupWise gateways.

NOTE: GroupWise gateways are legacy products that are not supported with the current GroupWise version.

Admin-Defined Fields

LDAP directories such as NetIQ eDirectory and Microsoft Active Directory include user information that is not associated to GroupWise user fields. By default, such LDAP fields are not displayed in the GroupWise Address Book. However, you can use the Admin-Defined Fields tool to map LDAP user fields to GroupWise fields so that they can be displayed in the GroupWise Address Book.

1 In the GroupWise Admin console, click **System > Admin-Defined Fields**.



LDAP fields that you associate with GroupWise fields here are available for use in all domains throughout your GroupWise system. You can also customize the GroupWise Address Book for individual domains. For instructions, see "Adding LDAP Fields to the Address Book" on page 70

2 Click the first field under the LDAP directory whose field you want to make available in GroupWise.

3 Select the LDAP property that you want to associated with the admin-defined field.

4 To remove an admin-defined field, click the field, then click **<Unused>**.

You are prompted for whether to remove the corresponding values from user records. This might be a time-consuming process.

5 Click **Yes** to clean up all obsolete references to deleted admin-defined fields in all user records.

or

Click **No** to perform the cleanup later.

At any time, you can click **Cleanup** to remove obsolete references to deleted admin-defined fields from all user records. It is a good practice to run **Cleanup** periodically to ensure that the admin-defined fields in the GroupWise Admin console match the admin-defined fields that appear in user records.

Administrators

The Administrators tool enables you to set up multiple GroupWise administrators with rights only to specific domains or post offices. For usage instructions, see Chapter 3, “GroupWise Administrators,” on page 45.

Calendar Publishing

The Calendar Publishing tool enables you to set up Calendar Publishing Hosts for publishing GroupWise user’s calendars to the Internet. For setup instructions, see “Setting Up the GroupWise Calendar Publishing Host” in the *GroupWise 18 Installation Guide*. For management instructions, see Part XVI, “Calendar Publishing Host,” on page 623.

Directory Associations

The Directory Associations tool enables you to associate manually created GroupWise users with an LDAP directory. It also enables you to change users’ directory associations from one LDAP directory to another. For example, you can change from NetIQ eDirectory associations to Microsoft Active Directory associations. For more information, see “Changing the LDAP Directory Association of Users” on page 466.

Document Viewer Agent

The Document Viewer Agent tool sets up DVA objects that are required when you add a DVA to an existing post office. For more information, see Chapter 36, “Scaling Your DVA Installation,” on page 363.

Email Address Lookup

You can use the Email Address Lookup tool to search for the GroupWise object (User, Resource, Group) that an email address is associated with. You can then view the object’s information. For more information, see “Ensuring Unique Email Addresses” on page 471.

Expired Records

You can use the Expired Records tool to view and manage the GroupWise user accounts that have an expiration date assigned to them.

For detailed information and instructions, see “Removing GroupWise Accounts” on page 474.

External System Synchronization

The External System Synchronization tool lets you automatically synchronize information between your system and an external GroupWise system that is connected to your system. For information about connecting GroupWise systems and keeping information synchronized between them, see “Using an External Domain to Connect GroupWise Systems” on page 112 and “Synchronizing User Information between External GroupWise Systems” on page 115.

Global Signatures

You can build a list of globally available signatures that can be automatically appended to messages sent by GroupWise client users. The global signature is appended to messages after any personal signatures that users create for themselves. For setup instructions, see "Adding a Global Signature to Users' Messages" on page 460.

Information

The Information tool tallies the number of objects in your entire GroupWise system, as well as the number of external objects that represent objects in other email systems that your GroupWise system is connected to. It also tallies the number of mailboxes and licenses in your entire GroupWise system. You can also run an audit report for your entire GroupWise system by using the Information tool.

You can also run audit reports on a post office basis. For more details about audit reports, see "Auditing Mailbox License Usage in the Post Office" on page 127.

Internet Addressing

By default, GroupWise uses a proprietary address format consisting of a user's ID, post office, and domain (*userID*.*post_office*.*domain*). After you install the GroupWise Internet Agent (GWIA), you can configure your GroupWise system to handle one or more formats of Internet email addresses. For setup instructions, see Chapter 29, "Managing Internet Domains, Addressing, and Access," on page 273.

LDAP Directories and Servers

The LDAP Servers tool lets you define the LDAP directories and servers that you want to use with your GroupWise system. You can use NetIQ eDirectory or Microsoft Active Directory with your GroupWise system. As needed, you can set up multiple servers to make the directory more accessible throughout your GroupWise system. For more information, see Chapter 6, "LDAP Directories and Servers in Your GroupWise System," on page 79

Licensing

A GroupWise license is required to run GroupWise past the 60 day evaluation period. If your license lapses, GroupWise mail is still delivered, but you are unable to make any changes to the administration. GroupWise Messenger and GroupWise Mobility Service also depend on the license. See the list below for information about what happens to Messenger and Mobility if the license expires:

- **GroupWise Messenger:** If the license lapses, Messenger agents stop running and a system broadcast is sent to all users telling them the license has expired.
- **GroupWise Mobility Service:** Mobility checks the state of the license and if the license has expired or there is an error, Mobility displays a banner in the Mobility Admin console with information about the error. If the license has expired and passed the 60 day grace period, Mobility blocks devices from connecting. Once the GroupWise license has been updated, restart Mobility to resume device connectivity. Mcheck can be used to view GroupWise maintenance information. Run MCheck and select option 1, then option 4.

We recommend that you configure the license during the installation, but you can configure it afterwards. If your GroupWise server has an Internet connection, follow the steps in Automatically Configure License. If it doesn't, follow the manual steps in Manually Configure License.

Automatically Configure License

If you did not configure your license during install, you can enter your Micro Focus customer center credentials in the GroupWise Admin Console:

1. In GroupWise Admin Console > **System** > **Licensing**, select **Enable**.
2. Enter your Micro Focus customer center user name and password.

   If applicable, select the site for your installation.

If you license gets updated again later, you can select **Check Now** to update the license information.

Manually Configure License

To manually enter the license, follow the steps below on a machine with access to the Internet and with Java installed:

1. In GroupWise Admin Console > **System** > **Licensing**, select **Update**.
2. Click on the **licensing tool** link to download the `gwlictool.jar` file.
3. Launch the **gwlictool.jar** file. If you have problems running the file, make sure that Java is set as the default application for `.jar` files on your computer.
4. Enter your Micro Focus customer center user name and password and click **Get License**.

   NOTE: If you downloaded the licensing tool following the steps above, the **System GUID** contains the information for your GroupWise system. If you obtained the tool another way, run the following command on the GroupWise server to get your System GUID:

   `gwadminutil dbinfo [path_to_your_groupwise_domain_folder]`

   ---

5. Click **Copy License** to copy the output to the clipboard and then paste it into the **Update License** pop up in the GroupWise Admin.

Legacy

If you upgrade your GroupWise system from GroupWise 2012 or GroupWise 8, you might have legacy GroupWise gateways that are no longer supported. The Legacy tool enables you to easily delete them from your GroupWise system.

In addition, after an upgrade, you might have software distribution directories that are no longer needed in GroupWise 18. The Legacy tool enables you to easily delete them. Starting in GroupWise 18, GroupWise client software is distributed to user workstations using Client Auto-Update. For more information, see "Using Client Auto-Update to Distribute the GroupWise Client Software" on page 583.

Link Configuration

GroupWise domains and post offices must be properly linked in order for messages to flow throughout your GroupWise system. You can use the Link Configuration tool to ensure that your domains and post offices are properly linked and to optimize the links if necessary. For detailed information and instructions, see Chapter 10, “Managing the Links between Domains and Post Offices,” on page 101.

Pending Operations

Pending operations are the results of administrative operations, such as adding GroupWise objects and modifying GroupWise object properties, that have not yet been permanently written to the appropriate GroupWise databases. While operations are pending, GroupWise data is not in a consistent state.

For example, you can maintain any domain’s objects you have administrative rights over. However, because a secondary domain owns its own objects, any operation you perform from the primary domain on a secondary domain’s objects must be validated by the secondary domain. While the operation is being validated, the Pending Operations dialog box displays object details and the pending operation.

While the operation is pending, the object is marked Unsafe in the primary domain database. The Operation field in the dialog box displays the pending operation. An unsafe object can have other operations performed on it, such as being added to a group; however, the object record is not distributed to other domains and post offices in the system until it is marked Safe.

All pending operations require confirmation that the operation was either successfully performed or could not be performed. If the operation was successful, the pending operation is removed from the list, the record is marked in the database as Safe, and the record is distributed to all other domains and post offices in your system. If the operation could not be performed, the pending operation remains in the list where you can monitor and manage it.

1. In the GroupWise Admin console, connect to the domain whose pending operations you want to view.

   See “Connecting to a Domain” on page 35.

2. Ensure the agents are running for the domain and/or post office where you are checking for pending operations

3. Click **System** > **Pending Operations**.

   While an operation is being validated, the Pending Operations dialog box displays the object and the operation waiting completion and confirmation.

4. For more detailed information, select the pending operation, then click **View**.

5. If conditions on the network have changed so that a pending operation might now succeed, select the pending operation, then click **Retry**.

6. If you want to cancel a pending operating that has not yet taken place, select the pending operation, then click **Undo**.

7. Click **Close** when you are finished viewing pending operations.

Record Enumerations

The Record Enumerations tool lets you look inside your GroupWise databases to view the contents on a record-by-record basis. This is very useful for troubleshooting database issues such as checking replication between domains and GroupWise systems.

For more information, see Chapter 47, "Troubleshooting Database Problems," on page 419.

Recover Deleted Account

If you have a reliable backup procedure in place, you can use the Recover Deleted Account tool to restore recently deleted user and resource accounts from the backup version of the GroupWise primary domain database. After the account has been re-created, you can then restore the corresponding mailbox and its contents to complete the process. Membership in groups and ownership of resources must be manually re-established.

For complete instructions, see "Recovering Deleted GroupWise Accounts" on page 428.

Restore Area Management

A restore area is a location you designate to hold a backup copy of a post office so that you or GroupWise users can access it to retrieve mailbox items that are unavailable in your live GroupWise system. The Restore Area Management tool lets you manage your GroupWise system's restore areas.

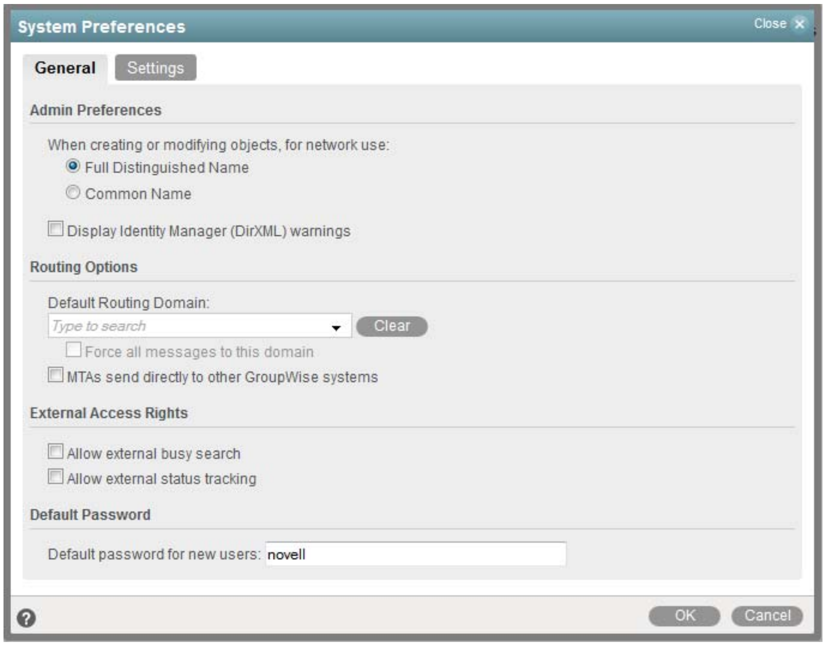
Detailed information for using restore areas is provided in "Restoring Deleted Mailbox Items" on page 425. Information about backing up post offices is provided in "Backing Up a Post Office" on page 421.

System Preferences

You can use the GroupWise system preferences to configure the defaults for various GroupWise system settings.

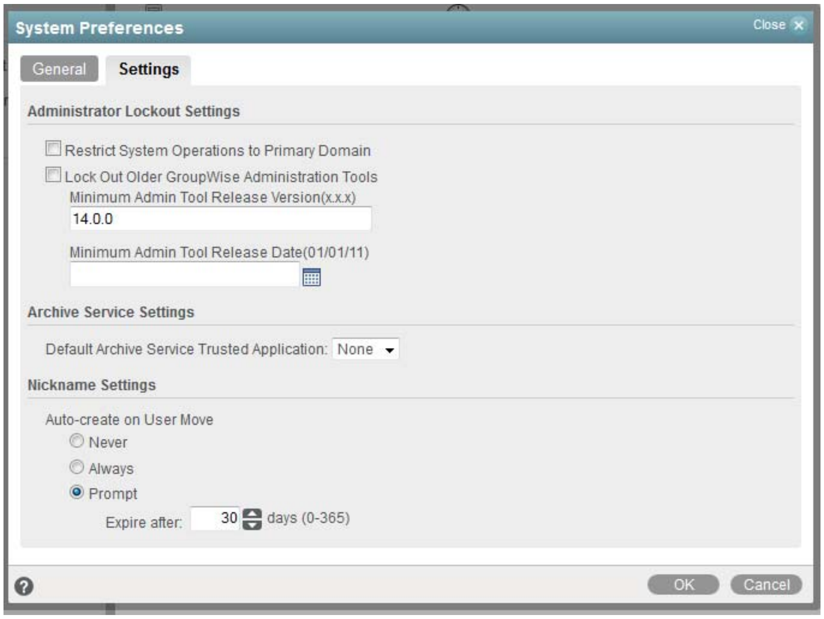
1 In the GroupWise Admin console, click **System > System Preferences**.

The **General** tab provides the following preferences:



- Admin Preferences: Controls how rights are assigned and what network ID format is used when creating new GroupWise users. By default, rights are assigned automatically and the fully distinguished name format is used.
- Routing Options: Controls default message routing for your GroupWise system. By default, no routing domain is assigned.
- External Access Rights: Controls the access that users on external GroupWise systems have to your GroupWise users' information. By default, Busy Search and status tracking information is not returned to users on external GroupWise systems.
- Default Password: Assigns a default password for new GroupWise user accounts. By default, you must manually assign a password for each GroupWise account you create.

The Settings tab provides the following preferences:



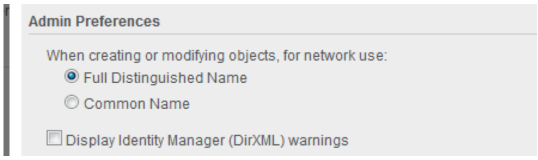
- Admin Lockout Settings: Controls access to the GroupWise administration functions in the GroupWise Admin console. By default, there are no restrictions.
- Archive Service Settings: Sets the default archive service for your GroupWise system. Archive services are third-party applications that can function as GroupWise trusted applications, such as NetMail Archive (http://www.netmail.com/products/m-archive-email-archiving.html). When you install an archive service to a server, the archive service is added to the list of archive service trusted applications that displays in the GroupWise Admin console.
- Nickname Settings: Controls how addressing is handled after you move a user from one post office to another. By default, nicknames representing old addresses are not automatically created when users are moved.

2 Change the system preferences as needed.

3 Click **OK** to save the changes.

Admin Preferences

1 In the System Preferences dialog box, click the **General** tab to modify any of the following options:



When Creating or Modifying Objects, For Network ID Use: These options are provided for backward compatibility for GroupWise post offices on NetWare servers. Starting in GroupWise 2012, NetWare is no longer a supported platform.

Display Identity Manager (DirXML) Warnings: The Identity Manager Driver for GroupWise provides data integration between GroupWise users and groups in eDirectory. For example, you can have an email account automatically created as soon as an employee is hired. The same driver can also disable an email account when a user is no longer active.

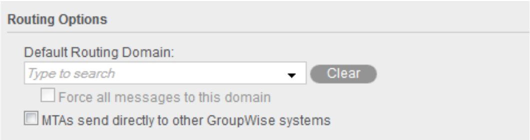
If you are using the Identity Manager Driver for GroupWise, some GroupWise operations that you perform in the GroupWise Admin console require you to take preliminary actions with the driver. For example, if you recover a deleted account, you need to stop the driver before recovering the account and restart it after the operation is complete.

This option enables you to receive a warning message whenever you perform a GroupWise operation in the GroupWise Admin console that is affected by the Identity Manager driver. The warning message includes instructions about the actions you need to take with the driver before continuing with the GroupWise operation. If you are using the Identity Manager Driver for GroupWise, we strongly recommend that you enable this option. If you are not using the driver, you can disable the option to avoid receiving unnecessary messages.

2 Click **OK** to save the changes.

Routing Options

1 In the System Preferences dialog box, click the **General** tab to modify any of the following options:



Default Routing Domain: If a domain's MTA cannot resolve a message's address, the message is routed to this default domain's MTA. The default domain's MTA can then be configured to handle the undeliverable messages. This might involve routing the message to another GroupWise domain or to an Internet address (by performing a DNS lookup). Browse to and select the GroupWise domain you want to use as the default routing domain.

Force All Messages to this Domain: This option applies only if you select a default routing domain. Select this option to force all messages to be routed through the default routing domain regardless of the links you have configured for your GroupWise system's domains.

MTAs Send Directly to Other GroupWise Systems: Select this option if you want all MTAs in your GroupWise system to perform DNS lookups and route messages out across the Internet. If you deselect this option, you can designate individual MTAs to perform DNS lookups and route messages to the Internet.

2 Click **OK** to save the changes.

External Access Rights

1 In the System Preferences dialog box, click the **General** tab to modify any of the following options:

Allow External Busy Search: Select this option to enable users in other GroupWise systems to perform Busy Searches on your GroupWise users' Calendars.

Allow External Status Tracking: Select this option to enable users in other GroupWise systems to receive message status information (such as whether a message has been delivered, opened, and so on) when messages arrive in your GroupWise system.

2 Click **OK** to save the changes.

Nickname Settings

A nickname is an additional GroupWise address that can be associated with a user, resource, or group. For background information, see "Manually Creating a Nickname for a User" on page 505.

1 In the System Preferences dialog box, click the **Settings** tab to modify any of the following options:

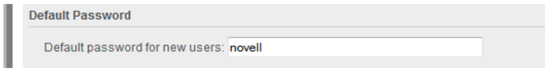
Auto-Create on User Move: Whenever you move a user, GroupWise can automatically create a nickname with the user's old post office. This enables messages sent to the old address to be automatically forwarded to the user's new address. Select whether or not you want GroupWise to never create nicknames, always create nicknames, or prompt you during the move process.

Expire After: This option applies only if you selected **Always** or **Prompt**. If you want the nickname to be automatically removed after a period of time, specify the time period (in days). Valid values range from 1 to 365 days. A setting of 0 indicates that the nickname will not be automatically removed.

2 Click **OK** to save the changes.

Default Password

1 In the System Preferences dialog box, click the **General** tab to modify any of the following options:

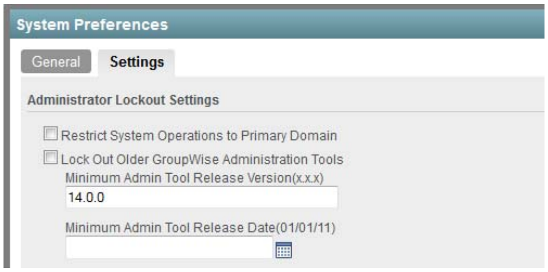


Default Password for New Users: Specify the default password you want assigned to new GroupWise user accounts.

2 Click **OK** to save the changes.

Admin Lockout Settings

1 In the System Preferences dialog box, click the **Settings** tab to modify any of the following options:



Restrict System Operations to Primary Domain: Disable this option to allow an administrator to perform system operations (**Tools** > **GroupWise System Operations**) when he or she is not connected to the primary domain. This option is enabled by default, which means that all operations except **Select Domain**, **Pending Operations**, **Software Directory Management**, and **Restore Area Management** are unavailable when connected to a secondary domain.

Lock Out Older GroupWise Administration Snap-Ins: Enable this option to prevent administrators from using older GroupWise administration tools (the GroupWise Admin console or ConsoleOne). You can override these system lockout settings for individual domains (Domain object > **GroupWise** > **Admin Lockout Settings**).

In the **Minimum Admin Tool Release Version (x.x.x)** field, specify the version number of the oldest GroupWise administrator tool that can be used to administer your GroupWise system.

In the **Minimum Admin Tool Release Date** field, select the date of the oldest GroupWise administration tool that can be used to administer your GroupWise system.

You can specify the minimum version, the minimum date, or both. If you specify both minimums, any administrator using snap-ins that are older than both minimums cannot use the GroupWise snap-ins. Default admin lockout settings can be overridden on individual domains as needed.

IMPORTANT: The specified release version and release date affect the Identity Manager GroupWise Driver as well as the GroupWise admin tool. If you are using Identity Manager with GroupWise, do not specify a release version or date that is newer than the release version and date of the Identity Manager GroupWise Driver that you are running.

---

2 Click **OK** to save the changes.

Archive Service Settings

When you use a message retention service with GroupWise, you have the option of associating an archive service with the message retention service. For more information, see Chapter 50, “Retaining User Messages,” on page 429.

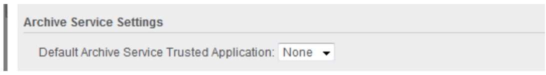
The message retention service and its associated archive service must be set up as a GroupWise trusted application. For instructions, see “Trusted Applications” on page 64.

Different archive services provide differing storage alternatives (memory, disk, or tape, for example) and differing alternatives for speed and cost. You can configure multiple archive services for your GroupWise system.

- “Selecting the System Default Archive Service” on page 61
- “Overriding the System Default Archive Service” on page 61

Selecting the System Default Archive Service

1 In the System Preferences dialog box, click the **Archive Service Settings** tab to select the system default archive service for your GroupWise system.



Archive Service Trusted Applications: Lists the third-party archive services that are available to your GroupWise system as trusted applications.

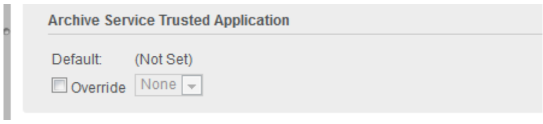
Select the archive service that you want to use as the default for your GroupWise system. You can override the system default on individual post offices.

2 Click **OK** to save your selection.

Overriding the System Default Archive Service

1 In the GroupWise Admin console, browse to and click the name of a post office.

2 Click the **Settings** tab.



3 In the **Default Archive Service Trusted Application** field, select **Override**.

4 Select the archive service for that post office, then click **OK**.

Time Zones

When you create a domain or post office, you select the time zone in which it is located. This ensures that GroupWise users in other time zones receive Calendar events and tracking information adjusted for local time.

The time zone list includes predefined definitions for each time zone. Most time zones include multiple definitions to account for different locations within the time zone. Each time zone definition allows you to specify the Daylight Saving Time dates and bias (1 hour, 30 minutes, etc.).

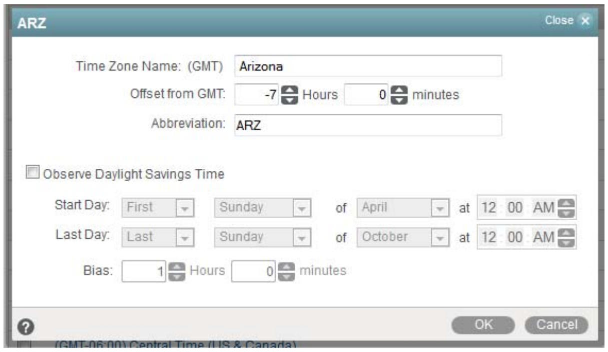
You can modify existing time zone definitions, add new definitions, or delete definitions.

- "Modifying a Time Zone Definition" on page 62
- "Adding a Time Zone Definition" on page 63
- "Deleting a Time Zone Definition" on page 64

Modifying a Time Zone Definition

1 In the GroupWise Admin console, click **System** > **Time Zones**.

2 Select the time zone to modify, then click **Edit** to display the Edit Time Zone dialog box.



3 Modify any of the following fields:

Time Zone Name: Provide a name for the time zone definition (for example, some of the major cities in the time zone). We suggest you include a reference (+ or -) to GMT, for example (GMT-07:00). The time zone list is sorted by the GMT offset.

Offset from GMT: Specify the hours and minutes that the time zone is offset from Greenwich Mean Time. The offset from GMT keeps your different locations synchronized. For example, if a conference call is scheduled for 4:00 p.m. June 1 in Salt Lake City, the call would appear on a schedule in Adelaide at 8:30 a.m. June 2. If you are in the western hemisphere (west of the Greenwich Meridian and east of the International Date Line) be sure the hour offset is negative (-). If you are in the eastern hemisphere (east of the Greenwich meridian and west of the International Date Line) be sure the hour offset is positive.

Abbreviation: Specify an abbreviation for the time zone. For example, the abbreviation for Atlantic Standard Time could be AST; the abbreviation for Atlantic Daylight Time could be ADT.

Observe Daylight Saving Time: If the time zone observes daylight saving time, click the **Observe Daylight Saving Time** box, then fill out the remaining fields.

Start Day: Select the week, day, month, and hour daylight saving time starts.

Last Day: Select the week, day, month, and hour daylight saving time ends.

Bias: Enter the number of hours and minutes that the clock changes at the daylight saving time start day, such as 1 hour or 1 hour 30 minutes.

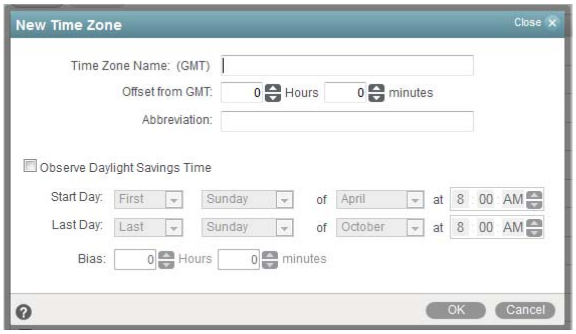
Example:
Start day: Second Sunday of March at 2:00 am.
Last day: First Sunday of November at 2:00 am.
Bias: 1 hour 0 minutes

4 Click **OK** to save the changes.

Adding a Time Zone Definition

1 In the GroupWise Admin console, click **System** > **Time Zones**.

2 Click **Add** to display the Add Time Zone dialog box.



3 Fill in the following fields:

Time Zone Name: Provide a name for the time zone definition (for example, some of the major cities in the time zone). We suggest you include a reference (+ or -) to GMT, for example (GMT-07:00). The time zone list is sorted by the GMT offset.

Offset from GMT: Specify the hours and minutes that the time zone is offset from Greenwich Mean Time. The offset from GMT keeps your different locations synchronized. For example, if a conference call is scheduled for 4:00 p.m. June 1 in Salt Lake City, the call would appear on a schedule in Adelaide at 8:30 a.m. June 2. If you are in the western hemisphere (west of the Greenwich Meridian and east of the International Date Line) be sure the hour offset is negative (-). If you are in the eastern hemisphere (east of the Greenwich meridian and west of the International Date Line) be sure the hour offset is positive.

Abbreviation: Specify an abbreviation for the time zone. For example, the abbreviation for Atlantic Standard Time could be AST; the abbreviation for Atlantic Daylight Time could be ADT.

Observe Daylight Saving Time: If the time zone observes daylight saving time, click the **Observe Daylight Saving Time** box, then fill out the remaining fields:

- **Start Day:** Select the day and time that daylight saving time starts.
- **Last Day:** Select the day and time that daylight saving time ends.
- **Bias:** Select the number of hours and minutes that the clock changes at the daylight saving time start day, such as1 hour or 1 hour 30 minutes.

4 Click **OK** to add the definition to the time zone list.

Deleting a Time Zone Definition

When you delete a time zone from the list, you can no longer select it for a domain or post office.

1 In the GroupWise Admin console, click **System** > **Time Zones**.

2 Select the time zone to remove from the list, click **Delete**, then click **Yes** to confirm the deletion.

Trusted Applications

Trusted applications are third-party programs that can log into POAs and GWIAs in order to access GroupWise mailboxes without needing personal user passwords. Trusted applications might perform such services as message retention or synchronization with mobile devices.

The Trusted Application tool allows you to edit and delete trusted applications that are available in your GroupWise system.

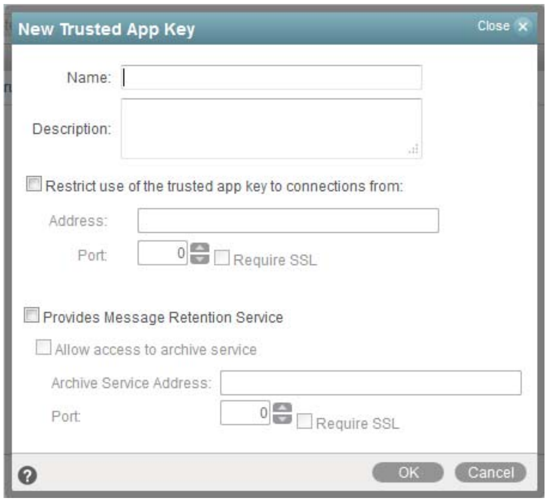
- “Creating a Trusted Application and Key” on page 65
- “Editing a Trusted Application” on page 66
- “Deleting a Trusted Application” on page 67

For information about developing and installing trusted applications, search for *GroupWise Trusted Application API* at the Micro Focus Developer Kit website (http://developer.novell.com/wiki/index.php/Category:Micro Focus_Developer_Kit). For security guidelines for managing trusted applications, see “Protecting Trusted Applications” on page 714

Creating a Trusted Application and Key

A trusted application key allows a third-party program to authenticate to the POA or the GWIA and obtain GroupWise information that would otherwise be available only by logging in to GroupWise mailboxes. You can create a trusted application and its associated key in the GroupWise Admin console for use with both Linux and Windows trusted applications.

1 In the GroupWise Admin console, click **System** > **Trusted Applications**, then click **New**.



2 Fill in the following fields as needed for your trusted application:

Name: Specify the name of the trusted application as you want it to be listed in the GroupWise Admin console.

Description: Specify a description for the trusted application.

TCP/IP Address: If you want to restrict the location from which the trusted application can run, specify the IP address of the server from which the application can run. To do so, click the **Edit** (pencil) button, then specify the IP address or DNS hostname of the trusted application's server.

If you want to allow the trusted application to be run from any server, do not specify an IP address or DNS hostname.

IMPORTANT: If you are creating the trusted application for use with the GroupWise Mobility Service, do not specify an IP address or DNS hostname. For more information, see "GroupWise Trusted Application" in the *GroupWise Mobility Service 18 Installation Guide*.

Requires SSL: Select this option to require a secure (SSL) connection between the trusted application and POAs and GWIAs.

Provides Message Retention Service: Select this option if the purpose of the trusted application is to retain GroupWise user messages by copying them from GroupWise mailboxes into another storage medium.

Turning on this option defines the trusted application as a Message Retention Service application. However, in order for GroupWise mailboxes to support message retention, you must also turn on the **Enable Message Retention Service** option in GroupWise Client Options (**Tools** > **GroupWise Utilities** > **Client Options** > **Environment** > **Retention**). You can enable individual mailboxes, all mailboxes in a post office, or all mailboxes in a domain by selecting the appropriate object (User, Post Office, or Domain) before selecting **Client Options**. For more information, see Chapter 69, "Setting Defaults for the GroupWise Client Options," on page 545.

For information about the complete process required to use a trusted application for message retention, see Chapter 50, “Retaining User Messages,” on page 429.

Allow Access to Archive Service: Select this option if your message retention service interacts with an archive service. Different archive services provide differing storage alternatives (memory, disk, or tape, for example) and differing alternatives for speed and cost. You can configure multiple archive services for your GroupWise system.

For more information about configuring GroupWise to work with an archive service, see “Archive Service Settings” on page 60.

Archive Service Address: If the trusted application for the message retention service uses the GroupWise Stubbing API (http://developer.novell.com/wiki/index.php/GroupWise_Stubbing), specify the IP address or DNS hostname of the server where the archive service is running. This allows the POA to interact directly with the archive service in support of the message retention service. The advantage to this configuration is that the archive service can be behind the firewall along with the POA. If retrieval is required, the POA accesses the archive service and provides the retrieved data to the GroupWise client.

If the message retention trusted application does not use the GroupWise Stubbing API, do not specify an IP address or DNS hostname. Without the Stubbing API, the trusted application communicates with the POA to create stubs for archived messages. The stubs contain the URLs for the archived messages. When a GroupWise user clicks the stub for an archived message, the GroupWise client accesses the URL to retrieve the archived message.

Archive Service Requires SSL: Select this option if you want to use a secure connection between the message retention service and the archive service.

Location for Key File: Browse to and select the directory where you want to create the trusted application key file.

Name of Key File: Specify the name of the trusted application key file to create. The third-party program must be designed to successfully access the trusted application key file where you create it.

3 Click **OK** to save the trusted application configuration information.

For information about how the POA handles trusted application processing of message files, see “Configuring Trusted Application Support” on page 154.

Editing a Trusted Application

You can edit a trusted application’s description, IP address, port, and SSL settings.

1 In the GroupWise Admin console, click **System** > **Trusted Applications** to display the Trusted Applications dialog box.

2 In the **Trusted Applications** list, select the application you want to edit, then click **Edit**.

3 Modify the fields as needed for your trusted application, then click **Close**.

For information about how the POA handles trusted application processing of message files, see “Configuring Trusted Application Support” on page 154.

Deleting a Trusted Application

1 In the GroupWise Admin console, click **System** > **Trusted Applications** to display the Trusted Applications dialog box.

2 In the **Trusted Applications** list, select the application you want to delete, click **Delete**, then click **Yes** to confirm the deletion.

User Import

The User Import tool imports users into your GroupWise system from an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory. The import process creates GroupWise accounts that are associated with the same user names that the users have in the directory.

For more information, see "Creating GroupWise Accounts by Importing Users from an LDAP Directory" on page 453.

User Move Status

You can use the User Move Status tool to track progress as you move users from one post office to another. Using the User Move Status tool, you can:

- List users that are currently being moved and filter the list by domain, post office, and object.
- View the current status of the move for each object and see any errors that have occurred.
- Immediately retry a move where some of the information on the user inventory list failed to arrive at the destination post office. By default, the POA retries automatically every 12 hours for seven days to move all the information included on the user inventory list.
- Stop the POA from continuing its automatic retries.
- Restart (from the beginning) a move that has stopped before successful completion.
- Refresh the list to display current move status and clear completed moves from the list.

For more information, see "Monitoring User Move Status" on page 464.

Standalone GroupWise Database Utilities

Although the GroupWise Admin console provides the primary administrative tool for managing your GroupWise system, additional standalone utilities are provided to meet specialized needs of GroupWise databases. These utilities perform tasks that might be necessary in environments where the GroupWise Admin console is not available.

- "GroupWise Check Utility (GWCheck)" on page 68
- "GroupWise Backup Time Stamp Utility (GWTMSTMP)" on page 68
- "GroupWise Administration Utility (GWAdminUtil)" on page 68
- "GroupWise Database Copy Utility (DBCOPY)" on page 68

GroupWise Check Utility (GWCheck)

GroupWise Check is a standalone version of the GroupWise Admin console Mailbox/Library Maintenance tool. Like the Mailbox/Library Maintenance tool, GroupWise Check checks and repairs GroupWise user, message, library, and resource databases. However, in addition to checking post office, user, and library databases, it also checks users' remote, caching, and archive databases.

For information about using GroupWise Check, see "GroupWise Check" on page 433.

GroupWise Backup Time Stamp Utility (GWTMSTMP)

The GroupWise Backup Time Stamp utility (GWTMSTMP) can be used to place a time stamp on a GroupWise user database to indicate the last time the database was backed up. If a user deletes an item from his or her mailbox and purges it from the Trash, the item is only deleted from the user's database if the time stamp shows that the item would have already been backed up. Otherwise, the item remains in the user's database until the database is backed up, at which time it is deleted from the working database.

For information about using the GroupWise Backup Time Stamp utility, see "GroupWise Backup Time Stamp Utility" on page 444.

GroupWise Administration Utility (GWAdminUtil)

The GroupWise Administration Utility (GWAdminUtil) enables you to perform security management, agent service management, and database management tasks on the command line. You can use GWAdminUtil to validate databases, correct physical problems in a domain or post office database, reclaim unused disk space, rebuild the user sorting index, and more.

For more information about the GroupWise Administration Utility, see "GroupWise Administration Utility" in the *GroupWise 18 Utilities Reference*.

GroupWise Database Copy Utility (DBCOPY)

The GroupWise Database Copy utility (DBCOPY) copies files from a live GroupWise system to a static location for backup. During the copy process, DBCOPY prevents the files from being modified, using the same locking mechanism used by other GroupWise programs that access databases. This ensures that the backed-up versions are consistent with the originals even when large databases take a substantial amount of time to copy.

For information about using the GroupWise Database Copy utility, see "GroupWise Database Copy Utility" on page 441.

5 GroupWise Address Book

The GroupWise Address Book plays a central role in a GroupWise user's experience with addressing messages. The default configuration of the GroupWise Address Book is often sufficient for a typical GroupWise system, but a variety of customization options are available to enable the GroupWise Address Book to meet user needs.

- "Customizing Address Book Fields" on page 69
- "Controlling Object Visibility" on page 72
- "Updating Address Book Information" on page 73
- "Controlling Users' Frequent Contacts Address Books" on page 74
- "Controlling Address Book Synchronization for Caching and Remote Client Users" on page 75
- "Publishing Email Addresses to the LDAP Directory." on page 76
- "Enabling Wildcard Addressing" on page 76
- "Adding External Users to the GroupWise Address Book" on page 78

NOTE: In addition to the administrator-controlled changes you can make to the Address Book, GroupWise users can make individual changes such as creating personal address books, sharing personal address books, and accessing LDAP address books. For information about the Address Book functionality available to users, see:

- "Contacts and Address Books" in the *GroupWise 18 Client User Guide*
- "Contacts and Address Books" in the *GroupWise 18 WebAccess User Guide*

Address books are not available in WebAccess Mobile.

Customizing Address Book Fields

The GroupWise clients displays specific fields in the GroupWise Address Book by default:

GroupWise Client	WebAccess
Name	Name
E-Mail Address	E-Mail Address
Title	
Office Phone Number	

NOTE: Address Book fields in GroupWise WebAccess are set permanently and cannot be changed by you or by users.

GroupWise client users can add more columns to their own Address Book. In the client, users right-click the Address Book column header, then select a column from the drop-down list or click **More Columns** to display a longer list of possible columns.

In the GroupWise Admin console, you can add columns to the list that is displayed in the GroupWise clients when users click **More Columns**. This is configured at the domain level.

NOTE: The Address Book configuration you establish becomes the default configuration for new GroupWise users in the domain. Changes to Address Book configuration do not affect existing users.

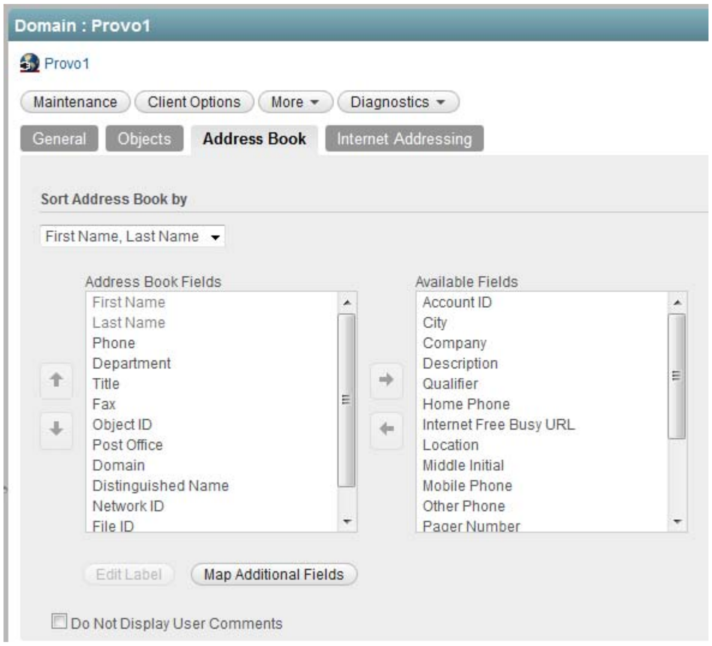
- "Adding LDAP Fields to the Address Book" on page 70
- "Changing the Default Sort Order" on page 71
- "Changing the Default Field Order" on page 71
- "Removing Fields from the Address Book" on page 71
- "Preventing the User Description Field from Displaying in the Address Book" on page 72

Adding LDAP Fields to the Address Book

Adding an LDAP directory field makes the field available in the GroupWise Address Book. Individual users can determine which available fields they want to display when they view the GroupWise Address Book in the GroupWise client.

1 In the GroupWise Admin console, browse to a click the name of a domain.

2 Click the **Address Book** tab.



The **Address Book Fields** list shows all fields that are available for selection in the Address Book in the GroupWise client.

The **Available Fields** list shows additional predefined GroupWise user fields that can be added to the Address Book. LDAP directories also include user information that is not associated to GroupWise user fields. You can use the **Map Additional Fields** button to map LDAP directory user fields to GroupWise fields so that they can be displayed in the GroupWise Address Book.

3 To add a field that is not displayed in the **Available Fields** list, click **Map Additional Fields** to open the Admin-Defined Fields tool. For more information, see "Admin-Defined Fields" on page 50.

4 In the **Available Fields** list, select the field you want to make available in the Address Book, then click the left-arrow to move it to the **Address Book Fields** list.

   The field is added to the bottom of the list. The Address Book displays the fields in the order they are listed.

5 If necessary, select the field, then use the up-arrow and down-arrow to move the field to the appropriate location in the list.

6 If the field is an Admin-defined field and you want to change how the field is labeled in the Address Book, select the field, click **Edit Label**, specify a new label in the **Address Book Label** field, then click **OK**.

   Administrator-defined fields are marked with an asterisk (*). You can only edit an Administrator-defined field that is in the **Address Book Fields** list.

7 Click **Save**, then click **Close** to return to the main Admin console window.

Changing the Default Sort Order

The sort order determines whether addresses in the Address Book are sorted by first name or last name. The sort order you establish becomes the default for the Address Book and remains in effect until individual users change it.

The preset default sort order for the Address Book is First Name/Last Name. You can change the default sort order to Last Name/First Name.

1 In the GroupWise Admin console, browse to and click the name of a domain.
2 Click the **Address Book** tab.
3 In the **Sort Address Book By** list, select the sort order you want to be the default.
4 Click **Save**, then click **Close** to return to the main Admin console window.

Changing the Default Field Order

The field order determines the order in which the GroupWise fields are displayed in the Address Book. The field order you establish becomes the default for the Address Book and remains in effect until individual users change the order.

1 In the GroupWise Admin console, browse to and click the name of a domain.
2 Click the **Address Book** tab.
3 In the **Address Book Fields** list, select a field whose position you want to change, then use the up-arrow and down-arrow to move the field to its new position.
4 Repeat Step 3 until you have established the field order you want.
5 Click **Save**, then click **Close** to return to the main Admin console window.

Removing Fields from the Address Book

If there are fields in the Address Book that are not used or that you don't want displayed to users, you can remove them.

1 In the GroupWise Admin console, browse to and click the name of a domain.
2 Click the **Address Book** tab.
3 In the **Address Book Fields** list, select the field you want to remove, then click the right-arrow to move the field to the **Available Fields** list.

The fields in the **Available Fields** list are not displayed in the Address Book.

4 Repeat Step 3 to remove additional fields you don't want to use.

5 Click **Save**, then click **Close** to return to the main Admin console window.

Preventing the User Description Field from Displaying in the Address Book

The GroupWise Address Book provides detailed user information as well as email addresses. A user's detailed information includes a comments field that displays the information stored in the User object **Description** field (User object > **General** > **Identification**). If you have included information in the **Description** field that you don't want displayed in the GroupWise Address Book, you can prevent the field's contents from being displayed.

TIP: To view a user's detailed information, including the comments field, in the Address Book, select the user's address, then click **View** > **Details**.

On the **Address Book** tab of the Domain object:

1. In the GroupWise Admin console, browse to and click the name of a domain.
2. Click the **Address Book** tab.
3. Enable the **Do Not Display User Comments** option.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Controlling Object Visibility

An object's visibility determines which post offices the object's information is distributed to. A post office's users can only see an object's information in the GroupWise Address Book if the object's information has been distributed to its post office.

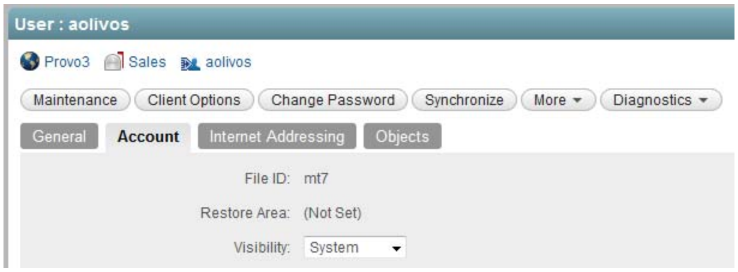
Visibility applies to the following objects:

- User
- Resource
- Group
- Nickname

IMPORTANT: Unlike the other objects listed above, nicknames that have been distributed to a post office do not actually appear in the post office's Address Book. Users must type the nickname's address in the message rather than select it from the Address Book.

To set an object's visibility:

1 In the GroupWise Admin console, browse to and click the name of the object, then click the **General** tab or the **Account** tab where the **Visibility** tab is located.



2 Set the visibility as needed:

- **System:** The object is visible in every post office Address Book throughout the system; if external system synchronization is turned on, it is also available for distribution to other GroupWise systems. This is the default for users, external users, resources, external resources, and nicknames.
- **Domain:** The object is visible only in the Address Book of the post offices located in the object's domain.
- **Post Office:** The object is visible only in the Address Book of the object's post office. This is the default for groups.
- **None:** The object is not visible in the Address Book of any post offices.

3 Click **Save**, then click **Close** to return to the main Admin console window.

Updating Address Book Information

Each post office database includes all the information displayed in the GroupWise Address Book that is stored in the domain. By keeping the information in the post office, the post office's users have quick access to it. Whenever changes are made in the LDAP directory that affect Address Book information, the information is replicated to each domain database and each post office database.

If information in a post office's Address Book is out-of-date or missing, you can synchronize the missing information with the LDAP directory or rebuild the post office database to obtain updated information from the domain.

- "Synchronizing Information" on page 73
- "Rebuilding the Post Office Database" on page 74

Synchronizing Information

The information for each object (user, resource, group, and so on) in the GroupWise Address Book is contained in the LDAP directory. When an object's information is incorrect in a post office's Address Book, you can synchronize the object's information in the Address Book with the information stored in the LDAP directory. This causes the correct information to be replicated to each domain and post office database in the GroupWise system. For instructions, see "Configuring User Synchronization for an LDAP Directory" on page 80.

Rebuilding the Post Office Database

If the post office Address Book is missing a lot of information, or if you are having other difficulties with information in the Address Book, you might want to rebuild the post office database. This causes all information to be replicated to the post office database from the domain database. For instructions, see "Rebuilding Domain or Post Office Databases" on page 398.

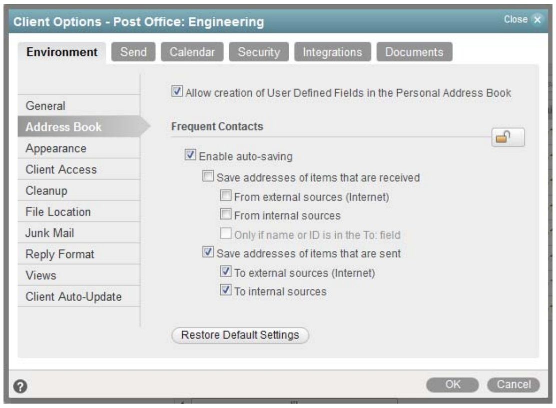
Controlling Users' Frequent Contacts Address Books

By default, email addresses of those to whom users send messages are automatically added to their Frequent Contacts address books. Users can also choose to automatically save email addresses of those from whom they receive messages. You can restrict the types of addresses that users can collect in their Frequent Contacts address books.

1 In the GroupWise Admin console, browse to and click the name of a domain, post office, or user.

2 Click **Client Options**

3 On the **Environment** tab, click **Address Book**.



4 With **Enable Auto-Saving** selected, adjust the auto-save options as needed.

Save Addresses of Items That Are Received: Select this option to allow users to automatically add external and internal email address from items that they receive to their Frequent Contacts address books. If desired, you can restrict users to collecting email addresses only if the user's name or email address appears in the **To** field, as opposed to the **CC** or **BC** fields.

Save Addresses of Items That Are Sent: Select this option to allow users to automatically add external and internal email address from items that they send to their Frequent Contacts address books.

or

Deselect **Enable Auto-Saving** to change the default so that email addresses are not collected unless users enable that functionality.

5 To prevent users from changing your Frequent Contacts address book settings, click the **Lock** button.

6 Click **OK** to save the Frequent Contacts address book settings.

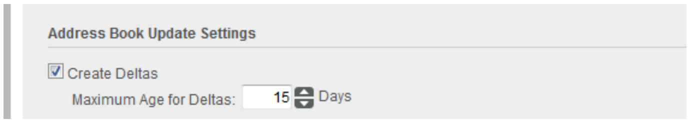
Controlling Address Book Synchronization for Caching and Remote Client Users

By default, the POA automatically updates the post office database (`wphost.db`) with changes to the Address Book as they occur. As a result, whenever a Caching or Remote client connects to the GroupWise system, it automatically downloads any updates to the Address Book that have occurred since the last time it connected. This means that Caching or Remote client users always have an up-to-date Address Book to work with.

Because the Address Book updates are stored as records in the post office database, this tool causes the post office database to grow in size as time passes. Therefore, in the GroupWise Admin console, you can specify the maximum number of days you want to store the incremental update records. The longer the incremental update records are stored, the larger the post office database becomes, which can impact available disk space and backup time. You can also disable this functionality, if necessary.

1 In the GroupWise Admin console, browse to and click the name of a post office.

2 Click the **Settings** tab



3 In the **Max Age for Address Book Updates** field, specify the number of days you want to retain Address Book update records.

The default is 15 days. The maximum number of days is 90.

4 (Optional) Deselect **Create Deltas for Address Book Updates** to disable this feature.

5 Click **OK** to save the setting.

Caching and Remote client users should not deselect **Refresh Address Books and Rules Every nn Days** because rules are still downloaded according to this schedule. Even if users do not want to download their rules, they still should not deselect this option because it turns off the Address Book delta sync. They can, however, set the option to a greater number of days to cause the download of the full Address Book to occur less frequently.

Publishing Email Addresses to the LDAP Directory.

The GroupWise databases and the LDAP directory both contain information about users' email address formats. When you change settings for users' GroupWise email addresses, you can publish the changes to the LDAP directory so that user email address information matches in both places.

1 In the GroupWise Admin console, click **System > Internet Addressing**.

2 Click the **Email Publishing**.

By default, users' preferred email addresses are published to eDirectory only in the format established in the **Preferred Address Format** field on the Addressing Formats tab. This publishes one email address per user in the format established for your GroupWise system.

3 Select additional options to publish additional email addresses, as needed.

4 Click **OK** to save the address publishing settings.

Enabling Wildcard Addressing

By default, users address messages by selecting users and groups from the Address Book. If you enable wildcard addressing, users can send items to all users in a post office, domain, GroupWise system, or connected GroupWise system by using asterisks (*) as wildcards in email addresses.

You can limit wildcard addressing to a specific level (system, domain, or post office) or allow unlimited wildcard addressing. The default is to limit the wildcard addressing to post office only, meaning that a user can use wild card addressing to send to all users on his or her post office only. You can change the default for individual users, post offices, or domains.

With wildcard addressing, the sender only sees whether the item was delivered to a domain, post office, or system (by viewing the item's properties). The properties do not show the individual user names or additional statuses. Recipients can reply to the sender only. Reply to All is unavailable.

- "Setting Wildcard Addressing Levels" on page 77
- "Wildcard Addressing Syntax" on page 77

NOTE: Wildcard addressing cannot be used for assigning shared folders or shared address books, granting proxy rights, performing busy searches, or sending routing slips.

Setting Wildcard Addressing Levels

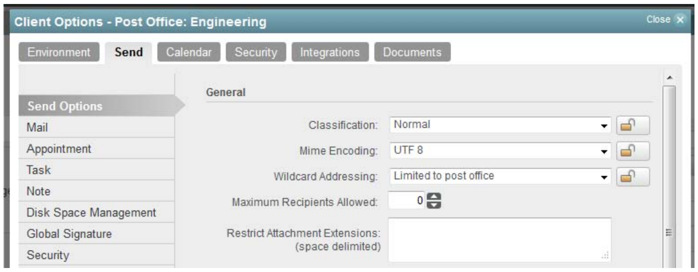
By default, wildcard addressing is enabled at the post office level for all users in your GroupWise system. You can change the level (post office, domain, or system) or disable wildcard addressing.

Wildcard addressing levels can be applied to a single user, to all users in a post office, or to all users in a domain.

To set wildcard addressing defaults:

1 In the GroupWise Admin console, browse to and click the name of a domain, post office, or user.

2 Click **Client Options**, then click the **Send** tab.



3 In the **Wildcard Addressing** list, select from the following options:

- **Not Allowed:** Select this option to disable wildcard addressing.
- **Limited to Post Office (Default):** Select this option to limit wildcard addressing to the user's post office. The user can use wildcard addressing to send items to users in his or her post office only.
- **Limited to Domain:** Select this option to limit wildcard addressing to the user's domain. The user can use wildcard addressing to send items to users in his or her domain only.
- **Limited to System:** Select this option to limit wildcard addressing to the user's GroupWise system. The user can use wildcard addressing to send items to all users in his or her system only. This excludes external users (users from other systems) who have been added to your GroupWise address book.
- **Unlimited:** Select this option to allow unlimited use of wildcard addressing. The user can use wildcard addressing to send to all users (including external users and non-visible users) defined in the GroupWise address book.

4 Click **OK** to save the changes.

Wildcard Addressing Syntax

The following table shows the syntax for wildcard addressing.

Wildcard Addressing Setting	To send an item to...	Type in the To field...
Limited to Post Office	All users in your post office	*
Limited to Domain	All users in your post office	*
	All users in your domain	*.*
	All users in another post office in your domain	*.*post_office*

Wildcard Addressing Setting	To send an item to...	Type in the To field...
Limited to System	All users in your post office	*
	All users in your domain	*.*
	All users in another post office in your domain	*.*post_office*
	All users in a post office in another domain	*.*post_office.domain*
	All users in another domain	*.*domain*
	All users in your GroupWise system	*.*.*
Unlimited	All users in your post office	*
	All users in your domain	*.*
	All users in a different post office in your domain	*.*post_office*
	All users in a post office in another domain. You can also use this for external post offices and external domains.	*.*post_office.domain*
	All users in a another domain. You can also use this for external domains.	*.*domain*
	All users in the GroupWise address book (all users in the same system, all external users, and all non-visible users)	*.*.*

Adding External Users to the GroupWise Address Book

The GroupWise Address Book lists all users that belong to your GroupWise system. When users receive incoming messages, the senders are added to users' Frequent Contacts Address Books to facilitate replying to users who are not included in the GroupWise Address Book. If necessary, you can configure GroupWise so that external (non-GroupWise) users appear in the GroupWise Address Book and are therefore available to all GroupWise users. For setup instructions, see "Using a Non-GroupWise Domain to Represent the Internet" on page 109

6 LDAP Directories and Servers in Your GroupWise System

You can define the LDAP directories and servers to use with your GroupWise system. You can use NetIQ eDirectory or Microsoft Active Directory with your GroupWise system. As needed, you can set up multiple servers to make the directory more accessible throughout your GroupWise system.

- "Setting Up an LDAP Directory" on page 79
- "Setting Up an LDAP Server" on page 81

Setting Up an LDAP Directory

LDAP directories such as NetIQ eDirectory and Microsoft Active Directory provide two important services to your GroupWise system:

- **User Synchronization:** User synchronization transfers modified user information from the LDAP directory to GroupWise for display in the GroupWise Address Book.

  The LDAP directory is the primary location for user information. User information that is synced from the LDAP directory cannot be modified in the GroupWise Admin console. GroupWise email addresses can optionally be synced into the LDAP directory.

  The MTA performs user synchronization for all users in the domain serviced by the MTA. The MTA then replicates the user information to all domains in your GroupWise system.

  For setup instructions, see "Configuring User Synchronization for an LDAP Directory" on page 80.
- **LDAP Authentication:** LDAP authentication requires that GroupWise users provide their directory (network login) passwords instead of GroupWise passwords in order to access their mailboxes.

  The POA performs LDAP authentication on behalf of the GroupWise client, the WebAccess Application, and the GWIA when these programs need to authenticate users to GroupWise.

  For setup instructions, see "Providing LDAP Authentication for GroupWise Users" on page 153.

Complete the following tasks to configure your LDAP directory for use with GroupWise:

- "Creating the LDAP Directory Object" on page 80
- "Configuring User Synchronization for an LDAP Directory" on page 80
- "Configuring LDAP Authentication" on page 81
- "Enabling Email Publishing" on page 81

Creating the LDAP Directory Object

To set up a new LDAP directory for use the GroupWise:

1 In the GroupWise Admin console, click **System > LDAP Servers**, then click **New Directory**.

2 Ensure that you know the required information for the LDAP directory that you want to use with GroupWise.

For more information about SSL, see "Server Certificates and SSL Encryption" on page 695.

IMPORTANT: If you want to use a limited rights user for the eDirectory sync user and want to import group objects, the sync user needs to have read rights to the CN attribute for group objects.

Also, if you plan on using LDAP Authentication with Active Directory and want to allow your users to change their Active Directory password through GroupWise, you must configure SSL for the LDAP directory object.

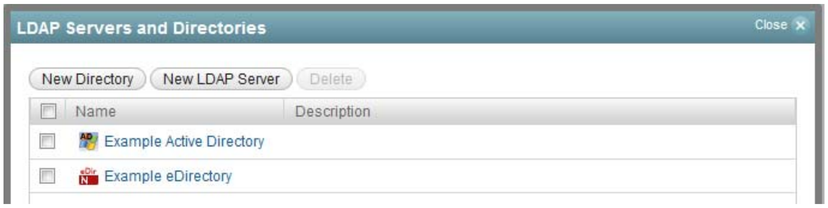
---

3 Fill in the fields, then click **Test Connection** to verify that you have provided accurate information about the LDAP directory.

4 Configure user synchronization.

For detailed instructions, see "Configuring User Synchronization for an LDAP Directory" on page 80.

5 Click **OK** to add the LDAP directory to GroupWise.



6 Click **Close** to return to the main Admin console window.

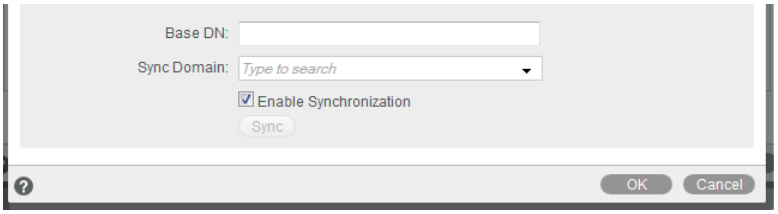
7 Skip to "Creating GroupWise Accounts by Importing Users from an LDAP Directory" on page 453.

Configuring User Synchronization for an LDAP Directory

When you import GroupWise users from an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory, you can select an MTA to synchronize updated user information from the LDAP directory into GroupWise. User synchronization is typically configured when the LDAP directory is established, but you can set it up or reconfigure it later as needed.

1 In the GroupWise Admin console, click **System > LDAP Servers**, then click the name of the LDAP directory.

User synchronization is configured in the bottom part of the General tab of the Directory object.



2 (Optional) In the **Base DN** field, specify the base context under which users to synchronize are located in the LDAP directory, for example:

```
ou=users,ou=org_unit,o=organization
cn=users,dc=server_name,dc=company_name,dc=com
```

3 In the **Sync Domain** field, select the domain whose MT you want to perform user synchronization with the LDAP directory.

4 Click **Sync** to send a task to the MTA to perform user synchronization.

5 Click **OK** to close the LDAP Servers and Directories dialog box.

Configuring LDAP Authentication

If you are planning to import users from your LDAP directory into your GroupWise system, you can use LDAP authentication instead of GroupWise authentication to provide mailbox access. For instructions, see "Providing LDAP Authentication for GroupWise Users" on page 153.

Enabling Email Publishing

If you are planning to import users from your LDAP directory into your GroupWise system, you can publish the GroupWise email addresses back to your LDAP directory. For instructions, see "Publishing Email Addresses to Your LDAP Directory" on page 471.

Setting Up an LDAP Server

You must configure one or more LDAP servers, in addition to an LDAP directory, when one or both of the following situations exist:

- You want to configure a pool of LDAP servers to provide redundancy for LDAP authentication.
- You want to provide GroupWise users in a remote location with a local LDAP server and directory replica to facilitate prompt LDAP authentication.

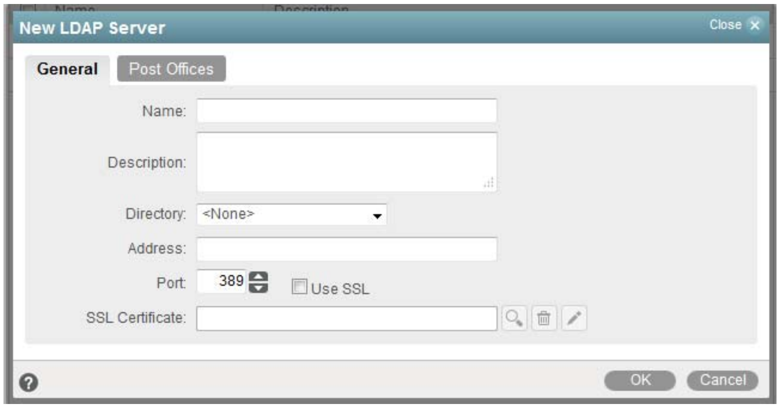
Add one of more LDAP servers to your GroupWise system, then configure a pool of LDAP servers for each post office.

- "Adding an LDAP Server" on page 82
- "Configuring a Pool of LDAP Servers" on page 83
- "Specifying Failover LDAP Servers (Non-SSL Only)" on page 83

Adding an LDAP Server

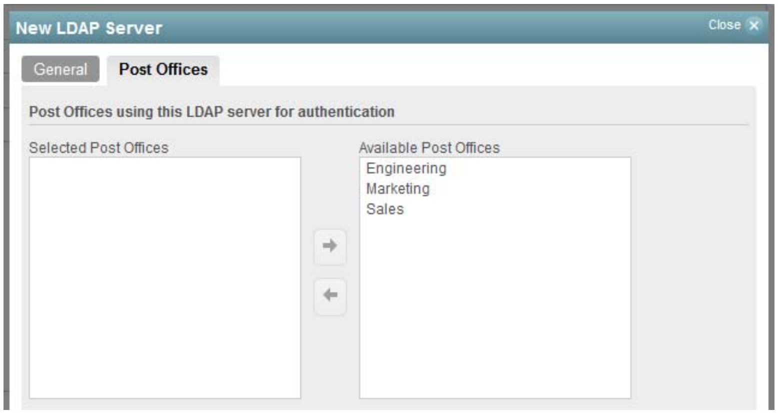
To add an LDAP server to make your LDAP directory more accessible:

1 In the GroupWise Admin console, click **System > LDAP Servers**, then click **New LDAP Server**.



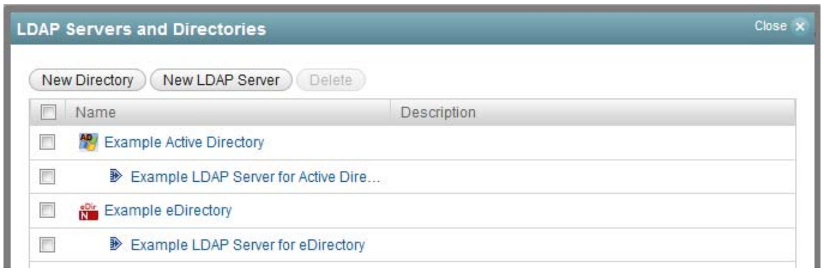
2 Ensure that you know the required information for the LDAP server that you want to set up for use with your LDAP directory.

3 Fill in the fields on the **General** tab, then click the **Post Offices** tab.



4 Select one or more post offices in the **Available Post Offices** list, then click the arrow button to move them into the **Selected Post Offices** list.

5 Click **OK** to add the new LDAP server to your GroupWise system.



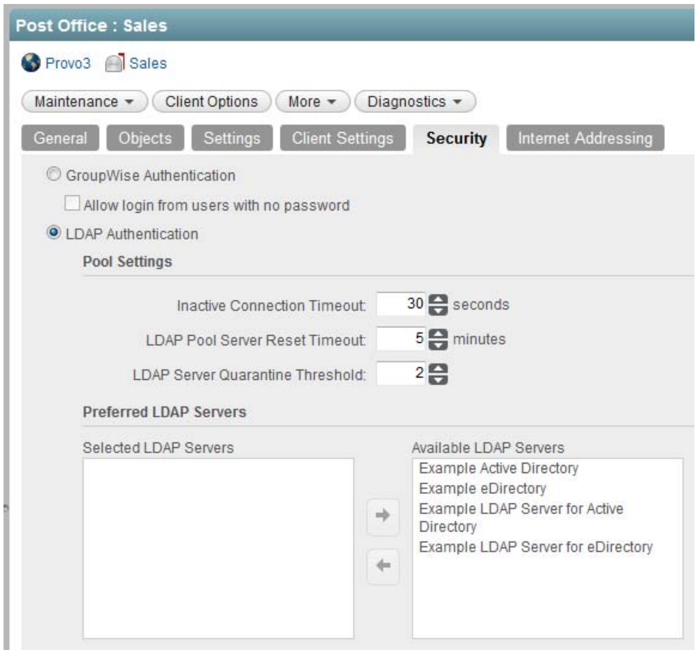
6 Click **Close** to return to the main Admin console window.

7 Continue with Configuring a Pool of LDAP Servers.

Configuring a Pool of LDAP Servers

When you configure multiple LDAP servers, all configured LDAP servers make up the initial LDAP server pool. By default, the POA can contact any server in the pool when authenticating a GroupWise user that belongs to a post office. This provides load balancing and fault tolerance because each LDAP server in the pool is contacted equally often by the POA.You might prefer that the POA for a post office first contact specific LDAP servers, contacting other servers in the pool only if none of the preferred LDAP servers are available.

1 In the GroupWise Admin console, ensure that you have more than one LDAP server set up for use with GroupWise.
2 Browse to and click the name of a post office, then click the **Security** tab.



3 Select **LDAP Authentication** to activate the pool settings.
4 (Optional) Adjust the pool settings as needed for your network environment.
5 Select one or more LDAP servers in the **Available LDAP Servers** list, then click the arrow button to move them into the **Selected LDAP Servers** list.
6 Click **OK** to save the security settings for the post office.

Corresponding Startup Switches: You can also use the --ldappoolresettime startup switch in the POA startup file to configure the timeout interval.

Specifying Failover LDAP Servers (Non-SSL Only)

If the POA does not need to use an SSL connection to your LDAP servers, you can use the --ldapipaddr switch to list multiple LDAP servers. Then, if the primary LDAP server fails to respond, the POA tries the next LDAP server in the list, and so on until it is able to access the LDAP directory. This provides failover LDAP servers for the primary LDAP server but does not provide load balancing, because the primary LDAP server is always contacted first.

1 In the GroupWise Admin console, ensure you have provided the basic LDAP information on the Post Office object **Security** tab.

For background information, see “Providing LDAP Authentication for GroupWise Users” on page 153.

2 Edit the POA startup file (*post_office*.poa) with an ASCII text editor.

   For more information about the POA startup file, see Chapter 20, “Using POA Startup Switches,” on page 183.

3 Use the --ldapipaddr startup switch to list addresses for multiple LDAP servers. Use a space between addresses.

   For example:

   /ldapipaddr-172.16.5.18 172.16.15.19 172.16.5.20

IMPORTANT: Do not include any LDAP servers that require an SSL connection. There is currently no way to specify multiple SSL key files unless you are using pooled LDAP servers. For more information, see “Configuring a Pool of LDAP Servers” on page 83.

---

4 Save the POA startup file, then exit the text editor.

5 Stop the POA, then start the POA so that it reads the updated startup file.

7 Multilingual GroupWise Systems

GroupWise is a multilingual email product that meets the needs of users around the world. The following sections provide guidance if your GroupWise system includes users who speak a variety of languages:

- "GroupWise User Languages" on page 85
- "GroupWise Administration and Agent Languages" on page 87
- "International Character Considerations" on page 88
- "MIME Encoding" on page 88
- "Multi-Language Workstations" on page 89

See also Chapter 71, "Supporting the GroupWise Client in Multiple Languages," on page 593.

GroupWise User Languages

The GroupWise client is available in 24 languages. All but three include spell checkers by default. Additional spell checkers are available in the open source community.

- "GroupWise Client Languages" on page 85
- "GroupWise Spell Checker Languages" on page 86

GroupWise Client Languages

Users can run GroupWise in the following languages:

Language	Code	Language	Code
Arabic**	AR	Italian	IT
Bulgarian	BG	Japanese	JA
Chinese - Simplified	CS	Korean	KO
Chinese - Traditional	CT	Norwegian	NO
Czech	CZ	Polish	PL
Danish	DA	Portuguese	PT
Dutch	NL	Russian	RU
English	EN	Slovak*	SK
Finnish	FI	Slovenian*	SL
French	FR	Spanish	ES
German	DE	Swedish	SV
Hungarian	HU	Turkish	TR

NOTE: Languages marked with an asterisk (*) are available for the GroupWise client, but not for GroupWise WebAccess. Languages marked with a double asterisk (**) are available for the GroupWise client and for GroupWise WebAccess in a desktop browser, but are not available on tablet devices or mobile devices where a more simple interface is used.

Language codes are used to identify language-specific files and directories. They are also used as the values of the client language (/l) startup option. Users can select the languages they want when they install the GroupWise client.

Users should have at least 200 MB available on their workstations to install the GroupWise client software in one language. Users need an additional 20 MB of disk space for each additional language they install.

By default, the GroupWise client starts in the language of the operating system, if it is available. If the operating system language is not available, the next default language is English. When you start the GroupWise client, you can use the /l startup switch to override the English default and select an interface language from those that have been installed.

The online help available in the GroupWise client is provided in all languages into which the client software is translated. The GroupWise client user guides available from the GroupWise client and on the GroupWise 18 Documentation website are translated only into the administration languages. If you try to access a user guide from a client that is running in a language into which the user guide has not been translated, you can select any of the available languages.

By default, the GroupWise client uses UTF-8 for MIME encoding. This accommodates the character sets used by all supported languages.

GroupWise Spell Checker Languages

By default, spell checkers are included for all GroupWise client languages except Chinese and Japanese. Spell checker variants are available for English, French, German, Norwegian, and Portuguese:

Language	Variant
English	Australia Canada United Kingdom United States
French	Canada France
German	Classic Spelling Germany Switzerland
Norwegian	Bokma Norsk
Portuguese	Brazil Portugal

For instructions on selecting the spell checker language variants, see “Selecting the Spell Checker Language” in the *GroupWise 18 Client User Guide*.

The open-source Hunspell (http://hunspell.sourceforge.net) and MySpell (http://en.wikipedia.org/wiki/MySpell) spell checkers provide many additional spell checker languages for use with the GroupWise client. The files required to install additional spell checkers can be downloaded from the following websites:

- Apache OpenOffice Dictionary Extensions (http://extensions.openoffice.org/en/search?f%5B0%5D=field_project_tags%3A157)
- Firefox Dictionary Extensions (https://addons.mozilla.org/en-US/firefox/language-tools/)

For instructions on using these open-source spell checkers with the GroupWise client, see "Adding a New Spell Checker Language " in the *GroupWise 18 Client User Guide*.

GroupWise Administration and Agent Languages

You can run the GroupWise Installation Wizard, administer your GroupWise system in the GroupWise Admin console, and run the GroupWise agents in the following languages:

Language	Code
English	EN
French	FR
German	DE
Portuguese	PT
Spanish	ES

Language codes are used to identify language-specific files and directories. They are also used as the values of the GroupWise agent /language startup switches.

When you select a language for a domain, it determines the sorting order for items in the GroupWise Address Book. This language becomes the default for post offices that belong to the domain. You can override the domain language at the post office level if necessary.

For example, if you set the domain and post office language to English, the Address Book items are sorted according to English sort order rules. This is true even if some users in the post office are running non-English GroupWise clients such as German or Japanese. Their client interface and Help files are in German or Japanese, but the sort order is according to English standards.

By default, the agents start in the language selected for the domain. If that language has not been installed, the agents start in the language used by the operating system. If that language has not been installed, the agents start in English. You can also use the /language agent startup switch to select the language for the agent to start in.

The POA also includes language-specific files in all client languages so that information returned from the POA to the GroupWise client, such as message status and undeliverable messages, is displayed in the language of the GroupWise client rather than the language in which the POA interface is being displayed.

Currently, the DVA is available only in English.

International Character Considerations

GroupWise client users have complete flexibility in the characters they use in composing messages. Accented characters used by various European languages and double-byte characters used by various Asian and Middle Eastern languages are all acceptable in the GroupWise client and can even be combined in the same message text.

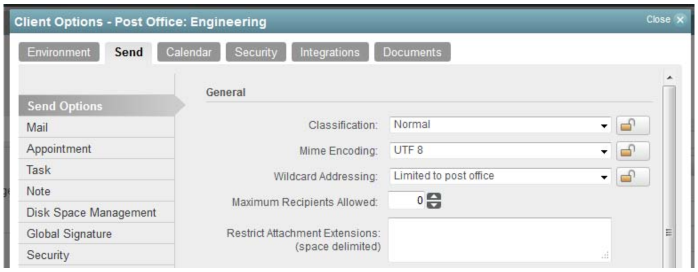
As an administrator, you must take the following limitations into account:

- Double-byte Asian and Middle Eastern characters should not be used in directory names and file names within your GroupWise system. This limitation is based on operating system capabilities. You should also not use double-byte characters in passwords. You can use double-byte characters in GroupWise user names, domain names, post office names, and so on.
- If you choose to use double-byte characters or extended characters such as accented characters in GroupWise user names or domain names, users must have Preferred E-mail IDs that contain only characters that are valid in the SMTP RFC. For instructions, see "Changing a User's Internet Addressing Settings" on page 472.

MIME Encoding

MIME (Multipurpose Internet Mail Extensions) encoding must be used when messages are sent across the Internet, so that characters display correctly for users on computers that are configured for different languages. In the GroupWise Admin console, you can set the default MIME encoding (for example, UTF-8, Windows Default, ISO Default, and so on) that is used by the GroupWise clients.

1. In the GroupWise Admin console, browse to and click the name of the domain, post office, or user where you want to change the maximum mailbox size.
2. Click the **Send** tab



3. In the **MIME Encoding** field, select the desired default MIME encoding.
4. Click **Save**, then click **Close** to return to the main Admin console window.

GroupWise users can override the default MIME encoding in GroupWise, as described in:

- "Changing the MIME Encoding for Email You Send" in the *GroupWise 18 Client User Guide*
- "Changing the MIME Encoding of a Message" in the *GroupWise 18 WebAccess User Guide*

The GroupWise client supports 24 character sets for MIME encoding. GroupWise WebAccess and the GroupWise Admin console support 16 character sets, marked with asterisks in the table below.

Languages/Alphabets	Character Sets
	Windows Default*

Languages/Alphabets	Character Sets
	ISO Default*
	UTF-8*
Arabic	Windows 1256*
Arabic	ISO 8859-6
Baltic	Windows 1257*
Baltic	ISO 8859-4
Central European	Windows 1250*
Central European	ISO 8859-2
Chinese Simplified	GB2312*
Chinese Traditional	Big 5
Cyrillic	KOI8-R*
Cyrillic	ISO 8859-5
Hebrew	Windows 1255*
Hebrew	ISO 8859-8
Japanese	ISO 2022-JP*
Japanese	Shift-JIS
Korean	EUC-KR*
Thai	Windows 874*
Turkish	Windows 1254*
Turkish	ISO 8859-9
Western European	Windows 1252
Western European	ISO 8859-1
Western European	ISO 8859-15

The GWIA also has options for controlling MIME encoding when messages are set to and from the Internet, as described in:

- GroupWise Admin console settings: "Determining Format Options for Messages" on page 298
- Startup switches: "Message Formatting and Encoding" on page 333

Multi-Language Workstations

If GroupWise users receive messages in multiple languages, their workstations need to be configured to handle the character sets used by these languages.

On Windows 8:

1. In the Control Panel, click **Clock, Language, and Region**.
2. Click **Change Location**, then click the **Keyboard and Languages** tab.

3 Click **How can I install additional languages**?

4 Follow the on-screen instructions to install the required language files.

On Windows 7:

1 In the Control Panel, click **Change Display Languages**.

2 In the **Display Language** box, click **Install/Uninstall Languages**.

3 Follow the on-screen instructions to install the required language files.

On Windows XP:

1 In the Control Panel, double-click **Regional and Language Options**, then click **Languages**.

2 If you receive messages in Chinese, Japanese, or other similar languages, select **Install Files for East Asian Languages**.

3 Click **OK** to install the required language files.

Domains

8 Creating a New Domain

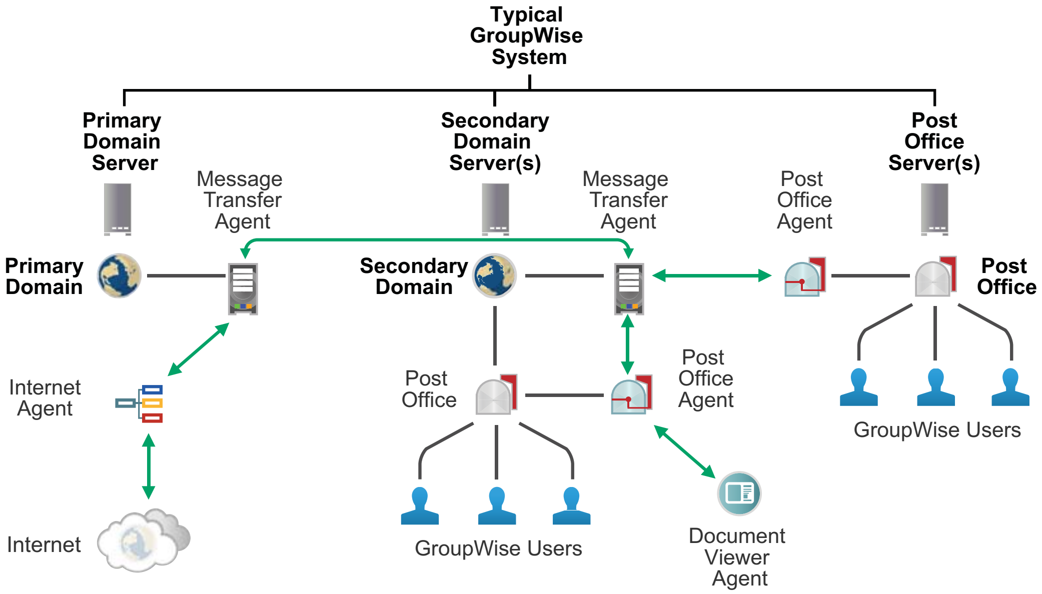
As your GroupWise system grows, you need to add new domains.

IMPORTANT: If you are creating a new domain in a clustered GroupWise system, see "Clustering" in the *GroupWise 18 Interoperability Guide*.

Understanding the Purpose of Domains

The domain functions as the main administrative unit for your GroupWise system. Each GroupWise system has one primary domain, which was created when you first installed GroupWise. All other domains that you add are secondary domains. The domain serves as a logical grouping of one or more post offices and is used for routing messages.

The following diagram illustrates the logical organization of a GroupWise system with multiple domains and post offices. All of the objects under the domain belong to that domain. All of the objects under a post office belong to that post office.



Messages are moved from user to user through your GroupWise system by the GroupWise agents. As illustrated above, each domain must have a Message Transfer Agent (MTA). The MTA transfers messages between domains and between post offices in the same domain. Each post office must have a Post Office Agent (POA). The POA delivers messages to users' mailboxes and performs a variety of post office and mailbox maintenance activities.

When you add a new domain to your GroupWise system, links define how messages are routed from one domain to another. When you add the first secondary domain, the links between the primary and secondary domains are very simple. As the number of domains grows, the links among them can become quite complex. Links are discussed in detail in Chapter 10, "Managing the Links between Domains and Post Offices," on page 101.

Physically, a domain consists of a set of folders that house all the information stored in the domain. The domain folder does not contain mailboxes or messages, but it does contain other vital information. For an overview, see "Information Stored in the Domain" on page 223. Domain folders can be located on Linux and Windows servers.

Creating a New Domain on a New Domain Server

You might have added a new secondary domain to your GroupWise system as you were creating it. Or you might be adding the first secondary domain to a small GroupWise system. In either case, the planning and procedure for adding a secondary domain on a new domain server is the same as if you were creating it in your initial GroupWise system.

The *GroupWise 18 Installation Guide* provides all of the information that you need to create a new secondary domain on a new domain server:

- "Planning a Domain"
- "Adding a Secondary Domain"

Creating a New Domain on an Existing Domain Server

Typically, you create a new domain on a new domain server, but if you need to create a new domain on an existing domain server, you can do so in the GroupWise Admin console.

1. In the GroupWise Admin console, click **Domains**, then click **New > Domain**.
2. Use the information that you gathered on the "Secondary Domain Worksheet" in the *GroupWise 18 Installation Guide* as you fill in the fields.

   Notice that, because you are creating the new domain on a server where a domain already exists, you cannot use the default port numbers.
3. Click **OK** to create the new domain.

What's Next

After you have added the new domain and started its MTA, you are ready to continue to expand and enhance your GroupWise system by:

- Configuring the Address Book for the new domain.

  See "GroupWise Address Book" on page 69.
- Adding post offices to the new domain.

  See "Post Offices" on page 117.
- Configuring the MTA for optimal performance.

  See "Message Transfer Agent" on page 221.
- Connecting domains and GroupWise systems across the Internet using the GWIA.

  See "Internet Agent" on page 263.
- Setting up GroupWise Monitor to monitor the GroupWise agents.

  See "Monitor" on page 637.

9 Managing Domains

As your GroupWise system grows and evolves, you might need to perform the following maintenance activities on domains:

See also Chapter 44, “Maintaining Library Databases and Documents,” on page 407.

Connecting to a Domain

Whenever you change domain information, it is efficient to connect directly to the domain before you begin making modifications. This enables the GroupWise Admin Service for the domain to write directly to the domain database (`wpdomain.db`). Performing administrative tasks in a domain while not connected to it increases the amount of administrative message traffic sent between domains.

To change your domain connection:

1 In the GroupWise Admin console, select the domain in the Connected Domain drop-down list.

Editing Domain Properties

After creating a domain, you can change some domain properties. Other domain properties cannot be changed.

1 In the GroupWise Admin console, browse to and click the name of a domain.

2 Click the objects (**Post Offices**, **Users**, **Groups**, and so on) to list objects of each type that belong to the domain.

3 Click the system tools (**Administrators**, **User Move Status**, and so on) to use the tool specifically in the context of the selected domain.

4 Click the Domain object tabs (**General**, **Address Book**, and **Internet Addressing**) to configure those aspects of the domain.

5 Click **Save**, then click **Close** to return to the main Admin console window.

Converting a Secondary Domain to a Primary Domain

You can change which domain is primary if it becomes more convenient to administer the primary domain from a different location. You can, however, have only one primary domain at a time. When you convert a secondary domain to primary, the old primary domain becomes a secondary domain.

This task requires direct file access to both domain databases. For that reason, it is not available in the GroupWise Admin console, which provides direct file access to one domain database through the Admin Service for that domain. Instead, you use the GroupWise Administration Utility (GWAdminUtil) to perform the task.

1 In the GroupWise Admin console, prepare to perform the conversion:

   1a Ensure that the MTA is running in both domains.

   1b Ensure that there are no pending operations for the primary domain.

   See “Pending Operations” on page 54.

2 On the secondary domain server, establish a direct connection to the primary domain server.

   On Linux, you can mount the file system. On Windows, you can map the drive.

3 Use the following command to convert the secondary domain into the primary domain

```
gwadminutil convert -d /path_to_secondary_domain -p /path_to_primary_domain
```

4 Copy the following files from the `certificates` folder in the old primary domain to the `certificates` folder in the new primary domain:

```
ca.crt
ca.key
ca.srl
ca.crl
issued/*
revoked/*
```

   The location of the `certificates` folder varies by platform:

Linux:	`/opt/novell/groupwise/certificates`
Windows:	`c:\Program Data\Micro Focus\GroupWise\gwadmin\certificates\`<GUID>

5 In the GroupWise Admin console, verify in the list of domains that the Primary Domain icon with the red underscore is now beside the new domain.

Deleting a Domain

You can delete a domain only when it no longer owns subordinate GroupWise objects. For example, you cannot delete a secondary domain if it still owns post offices. However, the MTA object and the associated MTA service are automatically deleted along with the Domain object.

1 In the GroupWise Admin console, connect to the primary domain.

2 Browse to and click the name of the domain to delete.

3 Delete any post offices that belong to this domain.

   See “Deleting a Post Office” on page 131.

4 Click **More > Delete** to delete the Domain object.

5 When prompted, click **Yes** to delete the corresponding domain folder structure.

The domain is deleted from your GroupWise system. The MTA and GWIA services associated with the domain are also deleted.

6 (Conditional) If applicable, uninstall the agent software from the server.

See the following sections in the *GroupWise 18 Installation Guide*:

- "Uninstalling the Linux GroupWise Agents and Applications"
- "Uninstalling the Windows GroupWise Agents and Applications"

Changing the MTA Configuration to Meet Domain Needs

Because the MTA transfers messages between domains and between post offices in the same domain, it affects the domain itself, local users in post offices belonging to the domain, and users who exchanges messages with local users in the domain. Proper MTA configuration is essential for a smoothly running GroupWise system. Complete details about the MTA are provided in Part V, "Message Transfer Agent," on page 221. As you create and manage domains, you should keep in mind the following aspects of MTA configuration:

- "Securing the Domain with SSL Connections to the MTA" on page 229
- "Restricting Message Size between Domains" on page 230
- "Optimizing TCP/IP Links" on page 243

Releasing a Domain from Your GroupWise System

When you release a secondary domain from your GroupWise system, it creates a new GroupWise system. The released secondary domain becomes the new primary domain in its own single-domain system.

This task requires direct file access to both domain databases. For that reason, it is not available in the GroupWise Admin console, which provides direct file access to one domain database through the Admin Service for that domain. Instead, you use the GroupWise Administration Utility (GWAdminUtil) to perform the task.

1 On your local machine, provide folder access to both the primary domain database and the secondary domain database.

2 Use the following command to release the domain:

```
gwadminutil release -p /path_to_original_primary_domain
                    -d /path_to_secondary_domain
                    -n name_of_new_gw_system
```

3 On the server where you performed the release, set up the GroupWise Super Admin user for the new GroupWise system:

```
gwadminutil setadmin /path_to_new_primary_domain
                     -a admin_user_name -p
```

4 On the new primary domain server, set up the GroupWise certificate authority for the new GroupWise system:

```
gwadminutil ca -d /path_to_new_primary_domain -g
```

5 Wait for replication of the new GroupWise system information from the primary domain to the post office.

On each post office server, you can use the following command to view the system name in the post office database:

```
gwadminutil dbinfo /path_to_post_office
```

6 On each post office server, install a new server certificate so that the local Admin Service can communicate with the primary domain Admin Service:

```
gwadminutil certinst -d /path_to_post_office
                     -ca ip_address_of_primary_domain_server:9710
                                                -a admin_user_name -p
```

For more information about the gwadmintuil command, see “Using the GroupWise Administration Utility” on page 39.

For more information about the GroupWise certificate authority, see “Using a Self-Signed Certificate from the GroupWise Certificate Authority” on page 695

Merging a Domain into Your GroupWise System

In order to merge an external domain into the local GroupWise system as a new secondary domain, the external domain must be the only domain in the other GroupWise system. For more information see “Releasing a Domain from Your GroupWise System” on page 97.

This task requires direct file access to both domain databases. For that reason, it is not available in the GroupWise Admin console, which provides direct file access to one domain database through the Admin Service for that domain. Instead, you use the GroupWise Administration Utility (GWAdminUtil) to perform the task.

1 Stop the GroupWise agents and the GroupWise Admin Service for both domains.

2 On your local machine, provide folder access to both the primary domain database and the secondary domain database.

3 Use one of the following commands to merge the external GroupWise domain into the local GroupWise system:

```
gwadminutil merge -p /path_to_local_primary_domain
                  -db /path_to_external_primary_domain

gwadminutil merge -mergesync -p /path_to_local_primary_domain
                  -db /path_to_external_primary_domain
```

The -mergesync option establishes external system synchronization between the local GroupWise system and any other external systems that were syncing with the external primary domain.

4 On the new secondary domain server, install a new server certificate so that the local Admin Service can communicate with the primary domain Admin Service:

```
gwadminutil certinst -db /path_to_secondary_domain
                     -ca ip_address_of_primary_domain_server:9710
                                                -a admin_user_name -p
```

5 Wait for replication of the domain information to the post office.

On each post office server, you can use the following command to view the owning domain name in the post office database:

```
gwadminutil dbinfo /path_to_post_office
```

6 On each post office server, install a new server certificate so that the local Admin Service can communicate with the primary domain Admin Service:

```
gwadminutil certinst -db /path_to_post_office
                     -ca ip_address_of_primary_domain_server:9710
                     -a admin_user_name -p
```

7 Start the GroupWise agents and the GroupWise Admin Service for both domains.

NOTE: The principles for merging GroupWise systems are the same for GroupWise 18 as they are for GroupWise 2012. For additional information on this topic, see “Merging GroupWise Systems” in the *GroupWise 2012 Multi-System Administration Guide*.

---

10 Managing the Links between Domains and Post Offices

When you create a new secondary domain in your GroupWise system or a new post office in a domain, you configure one direct link to connect the new domain or post office to a domain in your GroupWise system. For simple configurations, this initial link might be adequate. For more complex configurations, you must modify link types and protocols to achieve optimum message flow throughout your GroupWise system.

The following topics help you manage links between domains and post offices:

Understanding Link Configuration

In GroupWise, a link is defined as the information required to route messages between domains, post offices, and gateways in a GroupWise system. Initial links are created when domains, post offices, and gateways are created. The following topics help you understand link configuration:

Domain-to-Domain Links

The primary role of the MTA is to route messages from one domain to another. Domain links tell the MTA how to route messages between domains. Domain links are stored in the domain database (`wpdomain.db`). There are three types of links between source and destination domains:

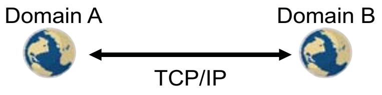
- "Direct Links" on page 101
- "Indirect Links" on page 102

As an alternative to configuring individual links between individual domains throughout your GroupWise system, you can establish a system of one or more routing domains. See "Configuring a Routing Domain" on page 231.

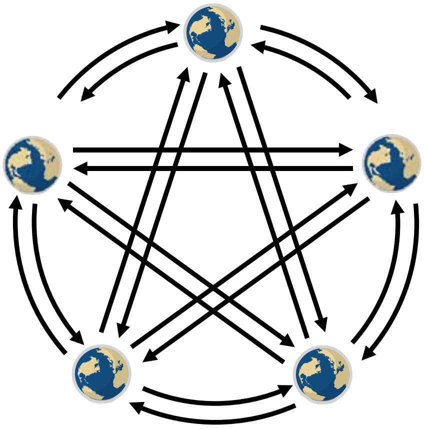
Direct Links

In a direct link between domains, the source domain's MTA communicates directly with the destination domain's MTA. If it is using a TCP/IP link, the source domain MTA communicates messages to the destination domain MTA by way of TCP/IP, which does not require disk access by the source MTA in the destination domain. This is the recommended configuration, and is the only option for domains on Linux.

If a Windows domain is using a mapped or UNC link, the source domain MTA writes message files into the destination domain MTA input queue, which does require disk access by the source MTA in the destination domain. For additional details about the configuration options for direct links, see "Link Protocols for Direct Links" on page 104.



Direct links can be used between all domains. This is a very efficient configuration but might not be practical in a large system.



Indirect Links

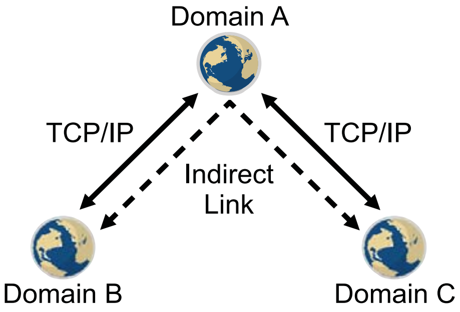
In an indirect link between domains, the source domain's MTA routes messages through one or more intermediate MTAs in other domains to reach the destination domain's MTA. In other words, an indirect link is a series of two or more direct links.

In large systems, direct links between each pair of domains might be impractical, so indirect links can be common. Properly configured links optimize message flow throughout your GroupWise system. A variety of indirect link configurations are possible, including:

- "Simple Indirect Links" on page 102
- "Star Configuration" on page 103
- "Two-Way Ring Configuration" on page 103
- "Combination Configuration" on page 103

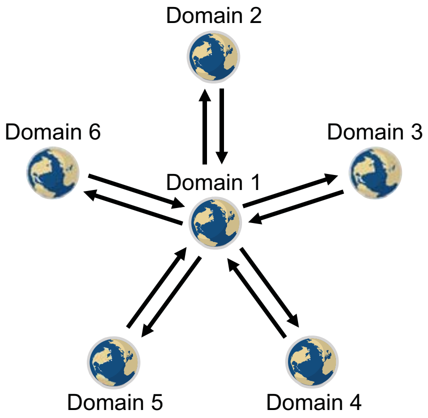
Simple Indirect Links

In simplest form, an indirect link can be used to pass messages between two domains that are not directly linked.



Star Configuration

In a star configuration, one central domain is linked directly to all other domains in the system. All other domains are indirectly linked to each other through the central domain.

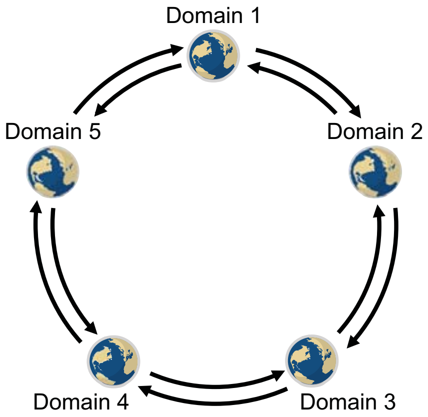


If you have more than ten domains, you might want to designate the central domain as a routing domain. The sole function of a routing domain is to transfer messages between other domains; it has no post offices of its own. See "Configuring a Routing Domain" on page 231.

The major drawback of the star configuration is that the central domain is a single point of failure.

Two-Way Ring Configuration

In a two-way ring configuration, each domain is directly linked to the next and previous domains in the ring and indirectly linked to all other domains in the system.



An advantage of the two-way ring configuration is that it has no single point of failure. A disadvantage is that, depending on the size of the system, a message might go through several domains before arriving at its destination. A two-way ring works well in a system with five domains or less because transferring a message never requires more than two hops.

Combination Configuration

These three basic link configurations can be combined in any way to meet the needs of your GroupWise system.

Domain-to-Post-Office Links

Between a domain and its post offices, all links must be direct links. There are no alternative link types between a domain and its post offices.

Link Protocols for Direct Links

The link protocol of a direct link between domains determines how the MTAs for the domains communicate with each other across the link. When you create a new domain, you must link it to an existing domain. This creates the initial domain-to-domain link.

Between a domain and a post office, the link protocol determines how the MTA transfers messages to the post office. Messages do not flow directly from one post office to another within a domain. Instead, they are routed through the domain. When you create a new post office, you must specify which domain it belongs to. This creates the initial domain-to-post-office link.

There are three link protocols for direct links between domains and between a domain and its post offices:

- "TCP/IP Links" on page 104
- "Mapped Links" on page 105
- "UNC Links" on page 105

NOTE: On Linux, TCP/IP links are required. On Windows, they are recommended.

TCP/IP Links

- "Domain-to-Domain TCP/IP Links" on page 104
- "Domain-to-Post-Office TCP/IP Links" on page 104

Domain-to-Domain TCP/IP Links

In a TCP/IP link between domains, the source MTA and the destination MTA communicate by way of TCP/IP rather than by writing message files into queue folders. The source MTA establishes a TCP/IP link with the destination MTA and transmits whatever messages need to go to that domain. The destination MTA receives the messages and routes them on to local post offices or to other domains as needed. During the process, message files are created in the `gwinprog` folder for backup purposes and are deleted when the TCP/IP communication process is completed.

Domain-to-Post-Office TCP/IP Links

In a TCP/IP link between a domain and a post office, you must configure both the POA and the MTA for TCP/IP. The source MTA establishes a TCP/IP link with the destination POA and transmits whatever messages need to go to that post office. The destination POA receives the messages and delivers them into mailboxes in the post office. During this process, message files are created in the POA input queue for backup purposes and are deleted when delivery is completed.

Mapped Links

Mapped links apply only to domains on Windows servers.

- "Domain-to-Domain Mapped Links" on page 105
- "Domain-to-Post-Office Mapped Links" on page 105

Domain-to-Domain Mapped Links

In a mapped link between domains, the location of the destination domain is specified in the following format:

`drive:\domain_folder`

The source MTA writes message files into its output queue at the following location:

`drive:\domain_folder\wpcsin`

The files are sent as input for the destination domain's MTA. Because drive mappings are changeable, you can move the domain folder structure, map its new location to the original drive letter, and the domain-to-domain link is still intact.

Domain-to-Post-Office Mapped Links

In a mapped link between a domain and a post office, the location of the post office is specified in the following format:

`drive:\post_office_folder`

The MTA writes message files into its output queue at the following location:

`drive:\post_office_folder\wpcsout`

The files are sent as input for the post office's POA. Because drive mappings are changeable, you can move the post office folder structure, map its new location to the original drive letter, and the domain-to-post-office link is still intact.

UNC Links

UNC links apply only to domains on Windows servers.

- "Domain-to-Domain UNC Links" on page 105
- "Domain-to-Post-Office UNC Links" on page 106

Domain-to-Domain UNC Links

In a UNC link between domains, the location of the destination domain is specified in the following format:

`\\server\volume\domain_folder`

The source MTA writes message files into its output queue at the following location:

`\\server\volume\domain_folder\wpcsin`

The files are sent as input for the destination domain's MTA. Because UNC paths represent absolute locations on your network, if you move the domain to a new location, you need to edit the link to match.

Domain-to-Post-Office UNC Links

In a UNC link between a domain and a post office, the location of the post office is specified in the following format:

*server**volume**post_office_folder*

The MTA writes message files into its output queue at the following location:

*server**volume**post_office_folder*\wpcsout

The files are sent as input for the post office's POA. Because UNC paths represent absolute locations in your network, if you move the post office to a new location, you need to edit the link to match.

Using the Link Configuration Tool

The Link Configuration tool helps you manage the links between the domains and post offices in your GroupWise system. The following topics help you perform basic link management tasks:

Accessing the Link Configuration Tool

The Link Configuration Tool is provided to help you change from default links to whatever link configuration best suits your GroupWise system.

1 In the GroupWise Admin console, click **System > Link Configuration** to display the Link Configuration tool.

The **Source** column lists all domains in your GroupWise system as the beginning point of links. The **Destination** column lists the end point of the links.

2 Click some domains in the **Source** column to see how the **Destination** column changes.

The following link type icons display beside domains in the **Destination** column:

Link Icon	Link Type/Status	Description
	Direct	Routes messages directly from the source domain to the destination domain.
	Indirect	Routes messages to the destination domain through one or more intermediate domains. In other words, an indirect link consists of two or more direct links.
	Gateway	Routes messages to the destination domain through a gateway link to another GroupWise system.
	Undefined	Stops message flow from the source domain to the destination domain.
	Pending Modification	Shows that you have changed link configuration information. You cannot make further changes until the link configuration information has been saved.

3 Continue with Editing Domain Links.

Editing Domain Links

In the Link Configuration Tool window, the right column allows you to edit the link between the selected domain in the Source column and the destination domain.

1. On the **Outbound Link** tab, click the **Link Type** drop-down list to change the link type between the source domain and the destination domain.

   The fields appropriate to each link type are provided.

2. Make changes as needed, then click **Save**.
3. To view the link from the point of view from the destination domain back to the source domain, click the **Inbound** tab.
4. Make changes as needed, then click **Save**.
5. Click **Close** when you are finished editing domain links.

11 Using an External Domain to Represent Another Email System

Your GroupWise system exists in a world of email systems.

A Non-GroupWise Domain object represents a non-GroupWise email system. You can set up a non-GroupWise domain in your GroupWise system so that users and groups in the other email system can be represented in the GroupWise Address Book.

An External Domain objects represents a domain in another GroupWise system. You can set up an external domain in your GroupWise system so that users, resources, and groups in the other GroupWise system can be represented in your GroupWise system. In addition, the other GroupWise system can set up your GroupWise system as an external domain as well. When both GroupWise systems have external domains to represent each other, the External System Synchronization tool can keep both GroupWise Address Books in sync as users, resources, and groups change over time.

Using a Non-GroupWise Domain to Represent the Internet

The GroupWise Address Book lists all users that belong to your GroupWise system. When users receive incoming messages, the senders are added to users' Frequent Contacts Address Books to facilitate replying to users who are not included in the GroupWise Address Book. If necessary, you can configure GroupWise so that external (non-GroupWise) users appear in the GroupWise Address Book and are therefore available to all GroupWise users.

Creating a Non-GroupWise Domain to Represent an Email System across the Internet

1. In the GroupWise Admin console, click **Domains**, then click **New** > **Non-GroupWise Domain**.
2. Fill in the fields:

   Domain Name: Specify a unique name for the non-GroupWise domain, such as Internet.

   Link to Domain: Select a domain where the GWIA is running.

   This links the external domain into your GroupWise system.

   By default, all messages sent to the non-GroupWise email system are routed through this domain. The domain's MTA routes the messages to the GWIA, which routes the messages to the Internet.

   Time Zone: Select the time zone where the other external email system is physically located.

   The time zone enables GroupWise to adjust appointment times according to local time.
3. Click **OK** to create the non-GroupWise domain to represent an external email system.

   The non-GroupWise domain is added to the list of domains in your GroupWise system.
4. Continue with Linking to the Non-GroupWise Domain.

Linking to the Non-GroupWise Domain

After you have created the non-GroupWise domain, you must modify the link between a domain where the GWIA is running and the non-GroupWise domain. This enables the GroupWise system to route all Internet messages to the MTA of this domain. The MTA can then route the messages to the GWIA, which sends them to the Internet.

To modify the link to the non-GroupWise domain:

1 In the GroupWise Admin console, click **System > Link Configuration** to display the Link Configuration tool.

2 Click the non-GroupWise domain to display it's links.

3 Configure the Gateway link:

   Link Type: Select **Gateway**.

   Gateway Link: Select the GWIA.

   Return Link: Displays the domain that the non-GroupWise domain is linked to.

4 Click **OK** to save the changes.

   The link from the GroupWise domain to the non-GroupWise domain displays as a gateway link.

5 Click **Save**, then click **Close** menu to exit the Link Configuration tool and save your changes.

6 Continue with Creating an External Post Office to Represent an Internet Host.

Creating an External Post Office to Represent an Internet Host

When you create an external post office to represent an Internet host, the post office name cannot be identical to the hostname because the period that separates the hostname components (for example, novell.com) is not a valid character for post office names. Therefore, you should choose a name that is closely related to the hostname.

To create an external post office:

1 In the GroupWise Admin console, click **Post Offices**, then click **New > External Post Office**.

2 Fill in the following fields:

   Name: Specify a name to associate the post office with the Internet host. Do not use the fully qualified hostname.

   Domain: Select the non-GroupWise domain.

   Time Zone: Select the time zone in which the Internet host is located.

3 Click **OK** to create the external post office.

4 Click the name of the external post office, then click the **Internet Addressing** tab.

5 If you want to override the GroupWise system allowed address formats, select **Override** under **Allowed Address Formats**, then select the allowed address formats for this Internet host.

6 Under **Internet Domain Name,** select **Override**, then specify the actual name of the Internet host that the external post office represents.

7 Click **Save**, then click **Close** to save your changes.

NOTE: If you have only a few users on some Internet hosts, you can create a single external post office for these users, then define their Internet domain names on the **General** tabs of the External User objects instead of on the External Post Office object.

---

8 Continue with Creating External Users to Represent Internet Users.

Creating External Users to Represent Internet Users

By creating external users to represent users in other email systems across the Internet, you can add them to the GroupWise Address Book for easy selection by GroupWise users.

To add an Internet user to an external post office:

1 In the GroupWise Admin console, browse to and click the name of the external post office, then click **New** to add a new external user.

2 In the **User Name** field, specify the exact user portion of the user's Internet address.

If the address is `jsmith@novell.com`, the portion you would specify is `jsmith`.

3 Click **OK** to create the external user.

4 Provide personal information about the external user:

4a Click the name of the new External User object.

4b Fill in the desired fields on the **General** tab.

Because the user is displayed in the GroupWise Address Book, you might want to define the user's first name and last name. This is especially important if the allowed address formats for the Internet host include first name and last name information.

4c Click **OK** to save the user's personal information.

5 Repeat Step 2a through Step 4 for each Internet user that you want to appear in the GroupWise Address Book.

6 (Conditional) As needed, use the same basic procedure to create external resources to represent resources in other email systems across the Internet.

7 Continue with Configuring External Users and Resources to Appear in GroupWise Busy Searches.

Configuring External Users and Resources to Appear in GroupWise Busy Searches

You can define the URL where free/busy schedule status is published for an external user or resource in a non-GroupWise email system. This enables GroupWise users to receive Busy Search results from this external user or resource along with Busy Search results from other GroupWise users.

1. In the GroupWise Admin console, browse to and click the name of the external user.
2. In the **Internet Free/Busy URL** field, specify the URL where free/busy schedule status for the user or resource is published, then click **OK**.

IMPORTANT: If the external email system is a Microsoft Exchange system, and if the users of the Exchange system want to synchronize user information with your GroupWise system, you can use the GroupWise Coexistence Solution to set up bidirectional synchronization between the GroupWise and Exchange systems. This solution populates the **Internet Free/Busy URL** field for you, as well as providing many other capabilities to facilitate GroupWise/Exchange coexistence. For more information, see the *GroupWise/Exchange Coexistence Guide*.

Using an External Domain to Connect GroupWise Systems

If you have two independent GroupWise systems, you can use the GWIA to connect the two systems. After the systems are connected, you can synchronize information between the two systems so that users from both systems appear in the GroupWise Address Book.

GroupWise System Connection Overview

When you connect two GroupWise systems, you connect two domains where GWIAs are running. These can be existing domains that have post offices, or you can create new domains whose only function is to provide an MTA and a GWIA for communicating with the other GroupWise system.

- In your local GroupWise system, define an external domain that represents the external GroupWise system. Configure a direct link from a local domain to the external domain. Define the link type as a Gateway link that uses the GWIA. This allows your local GroupWise system to deliver messages to the external GroupWise system.
- In the external GroupWise system, define an external domain that represents your local GroupWise system. Configure a direct link from a domain in the external GroupWise system to the external domain that represents your GroupWise system. Define the link type as a Gateway link that uses the GWIA. This allows the external GroupWise system to deliver messages to your local GroupWise system.

  If you do not have administrative rights in the other GroupWise system, you must coordinate with that administrator of the other GroupWise system.

After you have connected the two GroupWise systems, you use the External System Synchronization tool to exchange user information between the two systems. External System Synchronization constantly updates the GroupWise Address Books in both systems, so that local users can easily address messages to and access information about the users in the other GroupWise system.

Creating an External Domain

To create an external domain in your local GroupWise system to represent the other GroupWise system:

1 In the GroupWise Admin console, click **Domains**, then click **New** > **External Domain**.

2 Fill in the fields:

Domain Name: Specify a unique name that represents the other GroupWise system.

Link to Domain: Select a local domain where the GWIA is running.

By default, all messages sent to the other GroupWise system are routed through this local domain. The local domain's MTA routes the messages to the local GWIA, which connects to the external GWIA in the other GroupWise system.

Time Zone: Select the time zone where the other GroupWise system is physically located.

The time zone enables GroupWise to adjust appointment times according to local time.

Host: (Conditional) If the external domain represents a domain in the other GroupWise system where the MTA is directly accessible from your local GroupWise system, specify either the IP address or the DNS hostname of the external domain server. This provides the location of the domain database for the external domain.

In this configuration, the MTAs in the two GroupWise systems can directly exchange messages, rather than having the messages routed through GWIAs.

MTA MTP Port: (Conditional) If applicable, specify the port number on which the MTA in the external domain listens for messages. The default message transfer port for the MTA is 7100.

3 Click **OK** to create the external domain that links to the other GroupWise system.

The external domain is added to the list of domains in your GroupWise system.

4 Repeat Step 1 through Step 3 to define an external domain in the other GroupWise system that represents your local GroupWise system.

If you do not have administrative rights in the other GroupWise system, you must coordinate with that administrator of the other GroupWise system.

5 Continue with Linking to the External Domain.

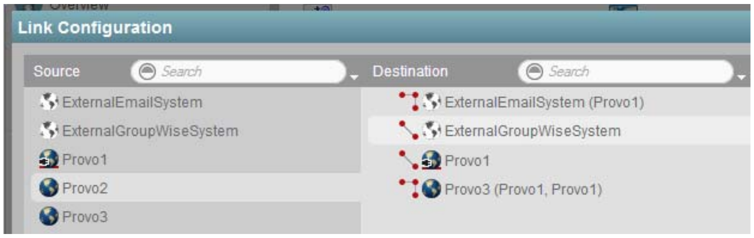
Linking to the External Domain

After you define a domain in the other GroupWise system as an external domain in your GroupWise system, you need to ensure that your system's domains have the appropriate links to the external domain.

The GWIA domain in your GroupWise system must have a Gateway link to the external domain. All other domains in your GroupWise system have indirect links to the external domain. These links were configured automatically when the external domain was created.

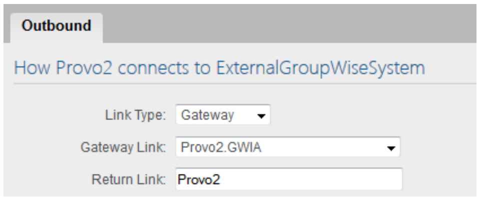
To configure the Gateway link for the domain where the GWIA communicates with the GWIA in the other GroupWise system:

1 In the GroupWise Admin console, click **System > Link Configuration** to display the Link Configuration Tool.



You can see that a domain in your local GroupWise system has a link to the external domain that represents the other GroupWise system.

2 Configure the link to the external domain:



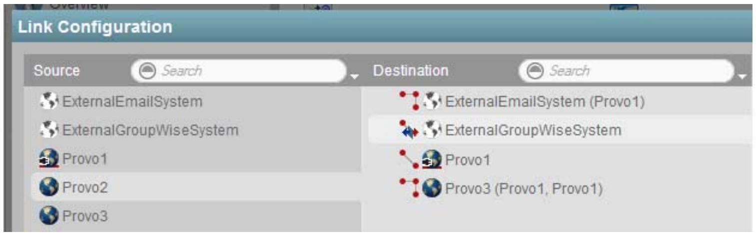
Link Type: Select **Gateway**.

Gateway Link: Select a GWIA to handle traffic to the external GroupWise system.

Return Link: Leave this set to the domain that is linked to the external domain.

3 Click **Save** to save the new link configuration.

The link between the local domain and the external domain is now listed as a Gateway link.



The rest of the domains in your GroupWise system should have indirect links to the external domain that represents the other GroupWise system.

4 Repeat Step 1 through Step 3 in the other GroupWise system to establish the Gateway link to your GroupWise system.

If you do not have administrative rights in the other GroupWise system, you must coordinate with that administrator of the other GroupWise system.

5 Continue with Synchronizing User Information between External GroupWise Systems.

Synchronizing User Information between External GroupWise Systems

The External System Synchronization tool lets you automatically synchronize information between your GroupWise system and another GroupWise system. For instructions on connecting GroupWise systems, see "Using an External Domain to Connect GroupWise Systems" on page 112.

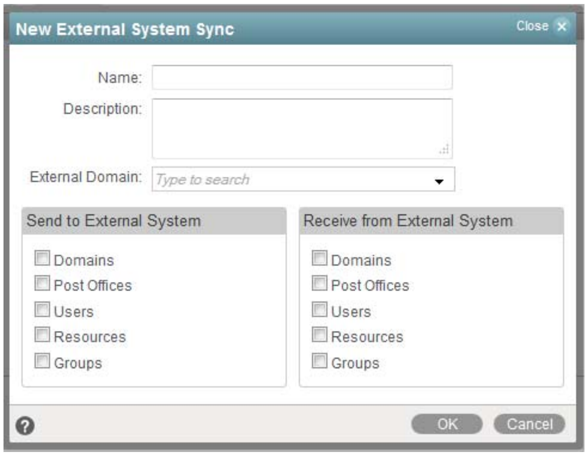
When you use the External System Synchronization tool, users, resources, and groups in each GroupWise system appear in the other system's GroupWise Address Book.

IMPORTANT: The External System Synchronization tool can synchronize GroupWise 8, GroupWise 2012, and GroupWise 18 systems. It cannot synchronize earlier GroupWise systems.

External System Synchronization lets you control what information (domains, post offices, users, resources, and groups) that you send to the external GroupWise system and what information you want to accept from the other GroupWise system. Any user, resource, and group information that you receive from the other GroupWise system is displayed in the GroupWise Address Book in your GroupWise system.

External System Synchronization must be set up in both GroupWise systems in order for it to work properly.

1 In the GroupWise Admin console, click **System > External System Synchronization**, then click **New** to create a new External System Synchronization profile.



2 Fill in the following fields:

Name: Specify the name of the other GroupWise system. The name must match the actual name of the other GroupWise system.

Description: (Optional) Enter a description for the other GroupWise system.

External Domain: Select the external domain that links to the other GroupWise system with which you are synchronizing information.

Send to External System: Select the information (Domains, Post Offices, Users, Resources, and Groups) that you want to send to the other GroupWise system during synchronization. Only the information that your GroupWise system owns is sent.

For example, if you have connected to another GroupWise system, and if its information is already contained in your GroupWise system as external domains, post offices, users, resources, and groups, that information is not sent

A user, resource, or group from your GroupWise system is added to the other GroupWise system only if its domain and post office exist in the other GroupWise system as an external domain and post office. Therefore, you should ensure that the **Domains** and **Post Offices** options are selected as well as the desired **Users**, **Resources**, and **Groups** options.

After the initial synchronization takes place, the domains and post offices exist in the other GroupWise system. You can then choose not to send domain and post office information going forward. However, if you add domains or post offices in your GroupWise system, or if you change the information for your existing domains and post offices, that information is not sent to the other GroupWise system until you select **Domains** and **Post Offices** again.

Receive from External System: Select the information (Domains, Post Offices, Users, Resources, and Groups) you are willing to receive from the other GroupWise system.

As with sending information, a user, resource, or group is added to your GroupWise system only if its domain and post office already exist as an external domain and post office in your GroupWise system. Therefore, you should ensure that you select the **Domains** and **Post Offices** options for at least the initial synchronization.

3 Click **OK** to add the other GroupWise system to the list of external GroupWise systems that you are synchronizing information with.

4 Click **Close** to exit the External System Synchronization tool.

Post Offices

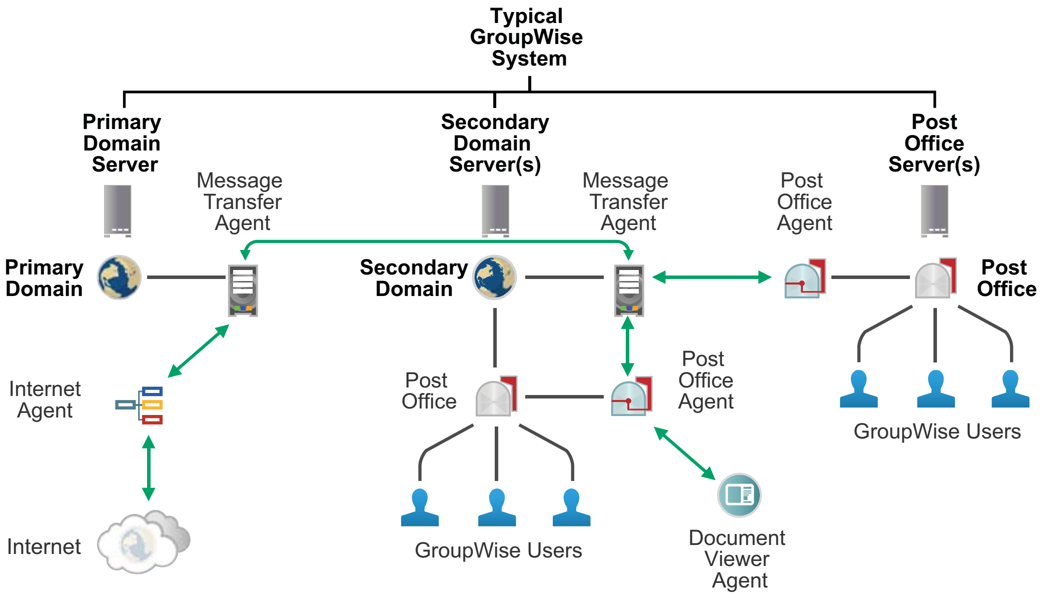
12 Creating a New Post Office

As your GroupWise system grows, you must add new post offices.

IMPORTANT: If you are creating a new post office in a clustered GroupWise system, see "Clustering" in the *GroupWise 18 Interoperability Guide* before you create the post office:

Understanding the Purpose of Post Offices

The post office serves as an administrative unit for a group of users and mailboxes.The following diagram illustrates the logical organization of a GroupWise domain with multiple post offices. The two post offices belong to the domain. All of the objects under each post office belong to that post office.



As illustrated above, each post office must have a Post Office Agent (POA) running for it. The POA delivers messages to users' mailboxes and performs a variety of post office and mailbox maintenance activities.

Physically, a post office consists of a set of folders that house all the information stored in the post office. The post office folder contains user mailboxes and messages, as well as other vital information. For an overview, see "Information Stored in the Post Office" on page 135.

Creating a New Post Office on a New Post Office Server

You added a new post office to your GroupWise system as you were creating it. The *GroupWise 18 Installation Guide* provides all of the information that you need to create a new post office on a new post office server:

- "Planning a Post Office"
- "Adding a Post Office"

Creating a New Post Office on an Existing Domain or Post Office Server

Typically, you create a new post office on a new post office server, but if you need to create a new post office on an existing domain server or post office server, you can do so in the GroupWise Admin console.

1 In the GroupWise Admin console, click **Post Offices**, then click **New > Post Office**.

2 Use the information that you gathered on the "Post Office Worksheet" in the *GroupWise 18 Installation Guide* as you fill in the fields.

IMPORTANT: If you are creating the new post office on a server where a post office already exists, you cannot use the default port numbers.

---

3 Click **OK** to create the new post office.

What's Next

After you have created the new post office and started its POA, you are ready to expand the post office by:

- Establishing post office security for the new post office.

  See "Configuring Post Office Security" on page 150.
- Adding users to the post office.

  See "Users" on page 451.
- Defining groups of users that GroupWise users can select when addressing messages.

  See "Groups" on page 481.
- Defining resources (for example, conference rooms or company cars) that users can schedule.

  See "Resources" on page 491.
- Defining libraries and setting up Document Management Services.

  See "Libraries and Documents" on page 511.
- Setting up the GroupWise client software so that GroupWise users can run the client from Windows workstations.

  See "Client" on page 533.
- Configuring the POA for optimal performance and security.

  See "Post Office Agent" on page 133.

13 Managing Post Offices

As your GroupWise system grows and evolves, you might need to perform the following maintenance activities on post offices:

See also Chapter 42, "Maintaining Domain and Post Office Databases," on page 395 and Chapter 48, "Backing Up GroupWise Databases," on page 421.

Proper database maintenance and backups allow recovery from accidental deletions. For more information, see "Restoring Deleted Mailbox Items" on page 425 and "Recovering Deleted GroupWise Accounts" on page 428.

Connecting to the Domain That Owns a Post Office

Whenever you change post office information, it is most efficient to connect directly to the domain that the post office belongs to before you begin making modifications. Performing administrative tasks in a post office while not connected to the post office's domain increases the amount of administrative message traffic sent between domains.

For instructions, see "Connecting to a Domain" on page 35.

Editing Post Office Properties

After creating a post office, you can change some post office properties. Other post office properties cannot be changed.

1. In the GroupWise Admin console, browse to and click the name of the post office.
2. Click the objects (**Users**, **Groups**, **Resources**, and so on) to list objects of each type that belong to the post office.
3. Click the system tools (**Administrators**, **User Move Status**, and so on) to use the tool specifically in the context of the selected post office.
4. Click the tabs (**General**, **Settings**, **Client Settings**, **Security**, and **Internet Addressing**) to configure those aspects of the post office.
5. Click **Save**, then click **Close** to return to the main Admin console window.

Managing Disk Space Usage in the Post Office

Many users are prone to save every message and attachment they ever receive. You can moderate this behavior by implementing disk space management:

Understanding Disk Space Usage and Mailbox Size Limits

The concept of mailbox size is different for GroupWise client users than it is for you as an administrator. Users are most interested in the functional size of their mailboxes; that is, the number of items that they can store in their mailboxes. Administrators are usually more concerned about the physical disk space that mailboxes occupy.

Functional mailbox size is computed by adding the bytes occupied by individual messages. Users are notified when they exceed the functional mailbox size limit that you have set for them. Users can then identify items to delete or archive.

- GroupWise client users can use **Tools > Check Mailbox Size** to list items in the Trash folder, the Sent Items folder, the Mailbox folder, the Work in Progress folder, and any personal items. Item size is displayed in bytes and the list is sorted from largest to smallest, to easily identify candidates for deletion or archiving.
- WebAccess users always have the **Size** column visible.

When users have deleted or archived sufficient items, their functional mailbox size limit problem is resolved.

As an administrator, you want to set functional mailbox size limits that are reasonable for users and that make efficient use of the physical disk space that you have available. You are more concerned about physical disk space usage in the post office. Physical disk space usage is much more complex than counting the bytes occupied by individual messages.

The following factors influence physical disk space usage:

- In a typical post office, 85% of disk space is occupied by attachments in the `offiles` folder structure. Attachments are compressed by 40% to allow more data to be stored in less space.
- A large message sent to multiple users in the same post office is only stored on disk once, but counts against mailbox size for all recipients. If it is sent to multiple post offices, a copy is stored in each post office
- A large group can cause even a small message to take up substantial disk space. If all recipients are in the same post office, only one copy is stored, but if there are recipients in multiple post offices, a copy is stored in each post office
- User databases (`userxxx.db` files) might contain large numbers of contacts and folders. Contacts and folders affect the size of the user databases, which have a maximum size of 4 GB, but do not count against the mailbox size for users.
- Shared folders count only against the owner's mailbox size, even though sharing with users in other post offices uses disk space in those post offices as well.
- A message is stored until the last recipient deletes and empties it. As a result, you might attempt to reduce post office disk space usage by reducing certain users' mailboxes, but disk space usage does not change. This can occur because large messages eliminated from the reduced mailboxes still exist in other mailboxes.

Because of the complexity of these factors, you might consider a progressive strategy to determine the appropriate functional mailbox limits for your users.

For a new post office, you could check the physical disk space occupied by the post office before users start accumulating email and initially set no functional mailbox limits. After a period of time (for example, a month), see how much the post office has grown. Run a report o assess the rate of mailbox growth. For instructions, see “Gathering Mailbox Statistics” on page 413. Then start setting functional mailbox limits based on user needs and available physical disk space.

- To set mailbox limits in a new post office, skip to “Setting Mailbox Size Limits” on page 123.
- For an existing post office, where users have never had functional mailbox limits set in the past, continue with Preparing to Implement Disk Space Management.

Preparing to Implement Disk Space Management

If you are implementing disk space management in an existing GroupWise system, you must begin by setting the initial size information on all users’ mailboxes.

To establish current mailbox size:

1. In the GroupWise Admin console, browse to and click the name of the post office.
2. Click **Maintenance > Mailbox/Library Maintenance.**
3. In the **Action** field, select **Analyze/Fix Databases**.
4. As options to the action, select **Content**, **Fix Problems**, and **Update User Disk Space Totals**.

   Ensure that all other options are deselected.
5. On the **Databases** tab, select **User**.

   Ensure that all other types of databases are deselected.
6. Click **OK**.

   After the POA has performed the task, current mailbox size information becomes available on each user’s mailbox. The information is updated regularly as the user receives and deletes messages.
7. To generate a report of current mailbox information, follow the instructions in “Gathering Mailbox Statistics” on page 413.
8. Repeat Step 1 through Step 7 for each post office where you want to implement disk space management.
9. Continue with Setting Mailbox Size Limits.

Setting Mailbox Size Limits

After initial size information is recorded on each user’s mailbox, you can establish a limit on the amount of disk space each user’s mailbox is allowed to occupy. You can set a single limit for an entire domain. You can set different limits for each post office. You can even set individual user limits if necessary.

If you are implementing disk space management in an existing GroupWise system where users are accustomed to unlimited disk space, you should warn them about the coming change. After you establish the mailbox size limits as described in this section, users whose mailboxes exceed the established limit cannot send messages until the size of their mailboxes is reduced. Users might want to manually delete and archive items in advance in order to avoid this interruption in their use of GroupWise.

To establish mailbox size limits:

1. In the GroupWise Admin console, browse to and click the name of a domain, post office, or user.

2 Click **Client Options**.
3 Click the **Send** tab, then click **Disk Space Management**.
4 Select **User Limits**.
5 Specify the maximum number of megabytes allowed for each user's mailbox.

   The maximum size limit that you can set for mailboxes is 4 TB.
6 Specify as a percentage the point where you want to warn users that their mailboxes are getting full.

   After users receive a warning message, they can continue to send messages until the size limit is reached. After the size limit is reached, users must reduce the size of their mailboxes in order to send additional messages.
7 (Optional) Specify in kilobytes the largest message that users can send.

IMPORTANT: By restricting message size, you can influence how fast users' mailboxes fill up. However, if users have valid reasons for sending messages that exceed this limit, the limit can become a hindrance to users getting their work done.

---

8 Click **OK** > **Close** to save the disk space management settings.
9 If you are adding disk space management to an existing GroupWise system where users' mailboxes are already over the desired size limit, continue with Enforcing Mailbox Size Limits.

   or

   If you are implementing disk space management in a new system where users have not yet begun to use their mailboxes, see "Using Mailbox Storage Size Information" in the *GroupWise 18 Client User Guide* to see how setting a mailbox size limit affects users' activities in the GroupWise client.

Enforcing Mailbox Size Limits

If existing GroupWise users are having difficulty fitting their mailboxes into the established mailbox size limits, you can assist them by reducing the size of their mailboxes for them.

When users archive and empty messages in their mailboxes, the messages are marked for removal from the database ("expired"), but the disk space that the expired messages occupied in the databases is retained and used again for new messages. As a result, archiving and deleting messages does not affect the overall size of the databases.

The Expire/Reduce Messages option of Mailbox/Library Maintenance enables you to expire additional messages and reduce the size of the databases by reclaiming the free space in the databases that is created when messages are expired. You should inform users before you run this process so they have a chance to archive or delete messages.

1 In the GroupWise Admin console, browse to and click the name of the post office.
2 Click **Maintenance > Mailbox/Library Maintenance.**
3 In the **Actions** drop-down list, click **Expire/Reduce Messages**.
4 In the **Action** field, select **Expire/Reduce**.
5 Set the **Expire** and **Reduce** options as desired, making sure that **Reduce Mailbox to Limited Size** is selected.
6 Click **OK**.

After the POA has performed the task, users mailboxes fit within the mailbox size limit you have established.

7. Repeat Step 1 through Step 6 for each post office where you want to reduce user mailboxes to the established mailbox size limit.

To see how setting a mailbox size limit affects user activities in the GroupWise client, see "Using Mailbox Storage Size Information" in the *GroupWise 18 Client User Guide*.

Restricting the Size of Messages That Users Can Send

By restricting message size, you can influence how fast user mailboxes fill up. However, if users have valid reasons for sending messages that exceed this limit, the limit can become a hindrance to users getting their work done.

For HTML-formatted messages, the MIME portion of the message counts in the message size. MIME files can be large. If a user cannot send an HTML-formatted message, he or she could use plain text instead, in order to decrease the size of the message so that it falls within the message size restriction.

There are four levels at which you can restrict message size:

- "Within the Post Office" on page 125
- "Between Post Offices" on page 125
- "Between Domains" on page 125
- "Between Your GroupWise System and the Internet" on page 126

Within the Post Office

You can use Client Options to restrict the size of messages that users can send within their local post office.

1. In the GroupWise Admin console, browse to and click the name of a domain, post office, or user.
2. Click **Client Options**.
3. Click the **Send** tab, then click **Disk Space Management**.
4. Select **User Limits**.
5. Specify in kilobytes the largest message that users can send.
6. Click **OK**, then click **Close** to save the maximum message size setting.

Between Post Offices

You can configure the POA to restrict the size of messages that it allows to pass outside the local post office. See "Restricting Message Size between Post Offices" on page 149 for setup instructions.

Between Domains

You can configure the MTA to restrict the size of messages that it allows to pass outside the local domain. See "Restricting Message Size between Domains" on page 230 for setup instructions.

Between Your GroupWise System and the Internet

You can configure the GWIA to restrict the size of messages that it allows to pass to and from your GroupWise system by setting the size limits in a customized class of service. See "Controlling User Access to the Internet" on page 279 for setup instructions.

Preventing the Post Office from Running Out of Disk Space

In spite of the best disk space management plans, it is still possible that some unforeseen situation could result in a post office running out of disk space. To prevent this occurrence, you can configure the POA to stop processing messages, so that disk space usage in the post office cannot increase until the disk space problem is resolved.

1. In the GroupWise Admin console, browse to and click the name of the post office.
2. Click the **Maintenance** tab, then adjust the settings in the **Disk Check Interval** and **Disk Check Delay** fields.

   For more information, see "Scheduling Disk Space Management" on page 156.
3. Click the **Scheduled Events** tab

   The Default Disk Check Event triggers a Reduce on user and message databases at 2048 KB (2 GB) and stop mail processing at 200 MB. You can edit the Default Disk Check actions so that all post offices are affected, or you can create a new set of Disk Check Event actions to assign to specific post offices.
4. Click **Create** to create a new scheduled event to handle an unacceptably low disk space condition.
5. Type a unique name for the new scheduled event, then select **Disk Check** as the event type.
6. In the **Trigger Actions At** field, specify the amount of free post office disk space at which to take preventive measures.
7. Click **New** to define your own disk check actions, then give the new action a unique name.
8. Configure the actions for the POA to take in order to relieve the low disk space condition.

   Use the **Results** or **Notification** tab if you want to receive notification about the POA's response to the low disk space condition.
9. Click **OK** to return to the **Create Scheduled Event** dialog box.
10. In the **Stop Mail Processing At** field, specify the amount of free post office disk space at which you want the POA to stop processing messages.
11. Click **OK** to create the new disk space management event and return to the **Scheduled Events** tab.
12. Select the new disk space management event.

    For additional instructions, see "Scheduling Disk Space Management" on page 156.
13. Click **Save**, then click **Close** to return to the main Admin console window.

An Alternative to Disk Space Management in the Post Office

If you want to place more responsibility for disk space management onto GroupWise client users, you can require that they run the client in Caching mode, where all messages can be stored on user workstations, or other personal locations, rather than in the post office. For instructions, see "Forcing Caching Mode" on page 127.

For an overview of Caching mode, see "Using Caching Mode" in the *GroupWise 18 Client User Guide*.

Forcing Caching Mode

You can force Caching mode for an entire domain, for specific post offices, or for individual users as necessary.

When you initially force caching mode, users' Caching mailboxes are identical with their Online mailboxes. However, as you employ disk space management processes in the post office and reduce the size of users' Online mailboxes, more and more of the users' mailbox items exist only in their Caching mailboxes.

IMPORTANT: Ensure that users understand their responsibilities to back up their Caching mailboxes. For more information, see "Backing Up Email" in the *GroupWise 18 Client User Guide*.

To force Caching mode:

1. In the GroupWise Admin console, browse to and click the name of a domain, post office, or user.
2. Click **Client Options**.
3. On the **Environment** tab, click **Client Access**.
4. In the **Client Login Mode** box, select **Force Use of Caching Mode**.
5. Click **OK** to save the Caching mode setting.

If you are helping existing users, who might have sizeable mailboxes, to start using Caching mode exclusively, you can configure the POA to respond efficiently when multiple users need to download their entire mailboxes for the first time. See "Supporting Forced Mailbox Caching" on page 149 for setup instructions.

Auditing Mailbox License Usage in the Post Office

You can run an audit report in a post office to see the following:

- Which mailboxes have been accessed using Full Licenses and which mailboxes have been accessed using Limited Licenses. A mailbox is considered to be a Full License mailbox if a user has logged in with the GroupWise client in the last 60 days.
- Which mailboxes are active (have been accessed at least one time), which ones have never been active, and which ones have been inactive for a specified period of time. The time period for measuring account activity is established by the **Log Accounts without Activity for Previous** setting when you run an audit report.
- Mailbox size, last login time, and last client type for all active mailboxes.

  The client type of each active license for each user is set by using **Client Options > Environment > Client Access** on Domain, Post Office, and User objects.

* Which mailboxes have been given Inactive status before the specified time period has passed.

  A GroupWise 18 mailbox can be given Inactive status on the User object **Account** tab. An older GroupWise mailbox cannot be given Inactive status.

A mailbox requires a Full License if it has been accessed by any of the following:

* The GroupWise client (`grpwise.exe`)
* GroupWise Notify (`notify.exe`) or GroupWise Address Book (`addrbook.exe`)
* GroupWise Address Book (`addrbook.exe`)
* A third-party plug-in to the GroupWise client API

A mailbox requires only a Limited License if access to it has been limited to the following:

* GroupWise WebAccess (including mobile devices)
* GroupWise client or WebAccess via the Proxy feature
* GroupWise client or WebAccess via the Busy Search feature
* A POP client
* An IMAP client
* A SOAP client such as GroupWise WebAccess or the GroupWise Mobility Service
* A third-party plug-in to the GroupWise SOAP protocol

A mailbox is considered active for licensing purposes if its owner has performed at least one of the following actions in the mailbox:

* Sending a message
* Opening a message
* Deleting a message
* Accessing the mailbox from a non-GroupWise client (for example, a POP3 email client) through the GWIA

A mailbox is considered inactive for licensing purposes even if its owner has performed one or more of the following actions (or similar actions):

* Starting and stopping the GroupWise client without doing anything in the mailbox
* Making changes under **Tools > Options**
* Creating, modifying, or deleting rules
* Granting proxy access so that a user other than the mailbox owner is performing tasks that would otherwise indicate an active mailbox

A GroupWise 18 mailbox can be marked **Inactive** on the User object **Account** tab. An older GroupWise mailbox cannot be marked **Inactive**.

To generate an audit report for the post office:

1. In the GroupWise Admin console, browse to and click the name of the post office.
2. Click **Maintenance > Mailbox/Library Maintenance.**
3. In the **Action** field, select **Audit Report**.
4. In the **Log Accounts without Activity for previous *xx* Days** field, select the number of days you want to use for the inactivity report.

The Mailbox/Library Maintenance feature uses the default setting (60 days) to flag all mailboxes that have not had any activity within the last 60 days. Select a different number to change the time period of the log you generate for the audit report. For example, you could generate a log report for the last 30 days. However, if you view the audit information by using **Tools > GroupWise Diagnostics > Information** on a System, Domain, or Post Office object, the information is always listed for the 60-day default time period.

5 (Conditional) If you want write the report to a log file, click the **Logging** tab, then specify a name for the log file.

   By default, the results are sent as an email message to the domain's notification user.

6 (Conditional) If you want to send the results to additional users:

   6a Click the **Results** tab.

   6b Specify the users' email addresses as a comma-delimited list in the **CC** field.

   6c Click **Message** to add personalized text to the message, then click **OK**.

7 Click **OK** to send the event to the POA.

   After the POA has performed the task, the audit report is sent to the users specified on the **Results** tab. The audit report lists all users who are currently considered inactive and flags those that have been inactive for longer than the number of days specified in the **Log Accounts without Activity for nn Days** field.

Audit reports are stored as part of the information available on Post Office and Domain objects in the GroupWise Admin console. Browse to and click the name of a Domain or Post Office object, then click **Diagnostics** > **Information**. The information stored on the Domain object is cumulative for all post offices in the domain for which audit reports have been run.

Audit reports can also be scheduled to run on a regular basis by properly configuring the POA to perform a Mailbox/Library Maintenance event. See "Scheduling Database Maintenance" on page 154.

Viewing Current Client Usage in the Post Office

The GroupWise Admin console can display the number of users who are using the GroupWise client. The client version is also displayed.

1 In the GroupWise Admin console, click **System > Information**.

   or

   Click the name of a post office or a domain, then click **Diagnostics > Information**.

2 Review the mailbox and license counts.

3 Click **OK** when you are finished.

Restricting Client Access to the Post Office

By default, the post office allows multiple versions of the GroupWise client to access it. Using the POA console, you can see the version number of each GroupWise client that logs in to the post office in Online mode. This information is displayed on the POA console's C/S Users page. For more information, see "Using the POA Console" on page 163.

IMPORTANT: Because the POA provides the version tracking and enforces the client lockout, this functionality applies only to GroupWise clients that are accessing the post office in Online mode, not in Caching mode.

To help you control which versions of the GroupWise client are being used to access the post office, you can specify a required GroupWise client version for the post office. Any version that does not match the required minimum version is locked out.

1 In the GroupWise Admin console, browse to and click the name of the post office.
2 Click the **Client Settings** tab.
3 Fill in the following fields:

   Minimum Client Release Version: Specify the version to use as the post office's preferred GroupWise client version. Any version that does not match the preferred version is highlighted on the POA console's C/S Users page. Older versions are shown in red, and newer versions are shown in blue. The version number syntax should match what is displayed in the GroupWise client's About GroupWise dialog box.

   Minimum Client Release Date: This field is available only if you specify a release version. You can use this field to associate an expected release date with the release version. The C/S Users page highlights any dates that do not match the one entered here.
4 Click **Save** to save the changes.

Securing the Post Office with LDAP Authentication

For user convenience, you can configure the post office for LDAP authentication through an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory. LDAP authentication enables users to use their LDAP (network) passwords to access their GroupWise mailboxes, rather than having separate GroupWise passwords.

The POA performs the LDAP authentication for users in the post office. For setup instructions, see "Providing LDAP Authentication for GroupWise Users" on page 153.

Disabling a Post Office

Disabling a post office restricts users from starting the GroupWise client and accessing the post office in Online mode. However, users who are already running the GroupWise client can continue to access the post office; after they exit, they cannot access the post office again until the post office is enabled.

A post office must be disabled if you are rebuilding the post office database (`wphost.db`). You might also want to disable a post office when you are doing a complete GroupWise system backup. That ensures that all data is consistent at the time of the backup.

1 In the GroupWise Admin console, browse to and click the name of the post office.
2 Click the **Client Settings** tab.
3 Select **Disable Logins**, then click **Save** to disable the post office.
4 (Conditional) To re-enable logins and make the post office available again, deselect **Disable Logins**, then click **Save** to re-enable the post office.

Deleting a Post Office

You cannot delete a post office until you have moved or deleted all objects that belong to it. However, POA object and the associated POA service are automatically deleted along with the Post Office object.

1. In the GroupWise Admin console, browse to and click the name of the post office to delete.
2. Move or delete any resources that still belong to the post office.

   See "Moving a Resource" on page 499 and "Deleting a Resource" on page 500. You must more or delete resources before users, because users who own resources cannot be deleted without assigning a new owner in the same post office.
3. Move or delete any users that still belong to the post office.

   See "Moving GroupWise Accounts" on page 462 and "Removing GroupWise Accounts" on page 474.
4. Delete any groups that still belong to the post office.

   See "Deleting a Group" on page 489.
5. Delete any libraries that still belong to the post office.

   See "Deleting a Library" on page 523.
6. Click **More > Delete** to delete the post office.
7. When prompted, click **Yes** to delete the corresponding post office folder structure.

   The post office is deleted from the domain. The POA and DVA services associated with the post office are also deleted.
8. (Conditional) If applicable, uninstall the POA software.

   See the following sections in the *GroupWise 18 Installation Guide*:
   - "Uninstalling the Linux GroupWise Agents and Applications"
   - "Uninstalling the Windows GroupWise Agents and Applications"

Changing POA Configuration to Meet Post Office Needs

Because the POA delivers messages to mailboxes, responds in real time to users in Online mode, and maintains all databases located in the post office, its functioning affects the post office and all users who belong to the post office. Proper POA configuration is essential for a smoothly running GroupWise system. Complete details about the POA are provided in Part IV, "Post Office Agent," on page 133. As you create and manage post offices, you should keep in mind the following aspects of POA configuration:

- "Securing the Post Office with SSL Connections to the POA" on page 152
- "Providing LDAP Authentication for GroupWise Users" on page 153
- "Configuring Intruder Detection" on page 153
- "Supporting IMAP Clients" on page 147
- "Supporting SOAP Clients" on page 148
- "Optimizing Client/Server Processing" on page 171
- "Scheduling Database Maintenance" on page 154

- “Configuring Nightly User Upkeep” on page 157
- “Restricting Message Size between Post Offices” on page 149

IV Post Office Agent

- Chapter 14, “Understanding Message Delivery and Storage in the Post Office,” on page 135
- Chapter 15, “Configuring the POA,” on page 143
- Chapter 16, “Managing the POA,” on page 159
- Chapter 17, “Monitoring the POA,” on page 163
- Chapter 18, “Optimizing the POA,” on page 171
- Chapter 19, “Managing Indexing of Attachment Content,” on page 177
- Chapter 20, “Using POA Startup Switches,” on page 183

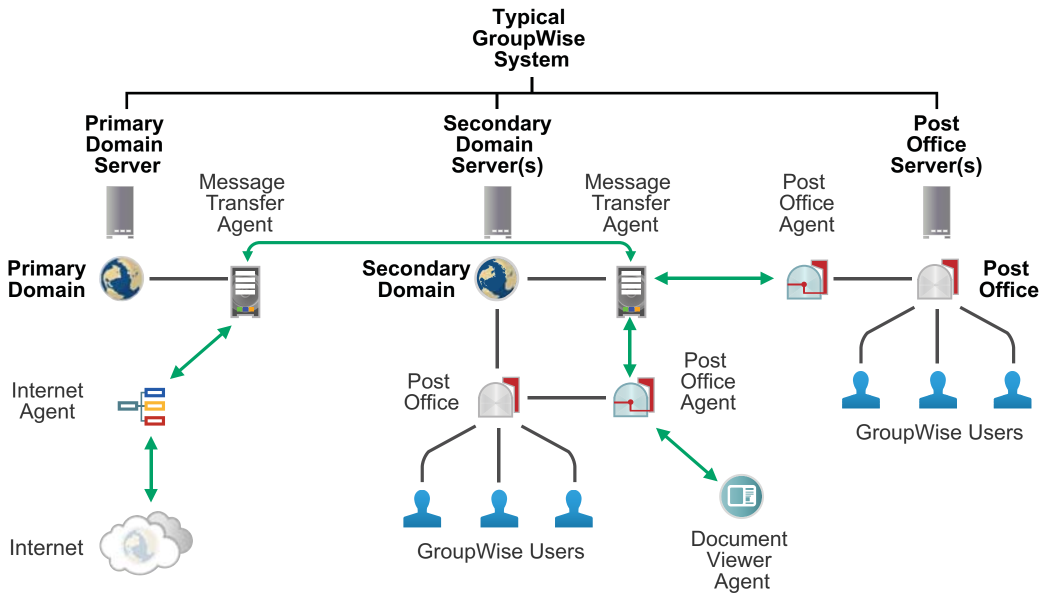
For a complete list of port numbers used by the POA, see Appendix A, “GroupWise Port Numbers,” on page 723.

For detailed Linux-specific POA information, see Appendix C, “Linux Basics for GroupWise Administration,” on page 735.

14 Understanding Message Delivery and Storage in the Post Office

The Post Office and the POA in Your GroupWise System

The post office serves as an administrative unit for a group of users and mailboxes. The POA delivers messages to users' mailboxes and performs a variety of post office and mailbox maintenance activities.



Post Office and POA Representation in the GroupWise Admin Console

In the GroupWise Admin console, post offices are listed under domains on the Overview page. POAs are listed under post offices.

Information Stored in the Post Office

The following types of information are stored in the post office:

IMPORTANT: All databases in the post office should be backed up regularly. How often you back up GroupWise databases depends on the reliability of your network and hardware. See "Backing Up a Post Office" on page 421.

Post Office Database

The post office database (`wphost.db`) contains all administrative information for the post office, including a copy of the GroupWise Address Book. This information is necessary for users to send messages to others in the GroupWise system.

Message Store

GroupWise messages are made up of three parts:

- **Message Header:** The message header contains addressing information including the sender's address, recipient's address, message priority, status level, and a pointer that links the header to the message body.
- **Message Body:** The message body contains the message text in an encrypted format and a distribution list containing user names of the sender and recipients.
- **File Attachments (optional):** File attachments can be any type of file that is attached to the message.

The message store consists of folders and databases that hold messages. The message store is shared by all members of the post office so only one copy of a message and its attachments is stored in the post office, no matter how many members of the post office receive the message. This makes the system more efficient in terms of message processing, speed, and storage space.

All information in the message store is encrypted to prevent unauthorized access.

The message store contains the following components:

- "User Databases" on page 136
- "Message Databases" on page 137
- "Attachments Folder" on page 137

User Databases

Each member of the post office has a personal database (`user`*`xxx`*`.db`) which represents the user's mailbox. The user database contains the following:

- Message header information
- Pointers to messages
- Folder assignments
- Personal groups
- Personal address books
- Rules
- Contacts
- Checklists

- Categories
- Junk Mail lists

When a member of another post office shares a folder with one or more members of the local post office, a "prime user" database (pu*xxxxx*.db) is created to store the shared information. The "prime user" is the owner of the shared information.

Local user databases and prime user databases are stored in the `ofuser` folder in the post office.

Message Databases

Each member of the post office is arbitrarily assigned to a message database (msg*nnn*.db) where the body portions of messages are stored. Many users in a post office share a single message database. There can be as many as 255 message databases (numbered 0 through 254) in a post office. Message databases are stored in the `ofmsg` folder in the post office.

Outgoing messages from local senders are stored in the message database assigned to each sender. Incoming messages from users in other post offices are stored in the message database that corresponds to the message database assigned to the sender in his or her own post office. In each case, only one copy of the message is stored in the post office, no matter how many members of the post office it is addressed to.

Attachments Folder

The attachments folder (`offiles`) contains subfolders that store file attachments, message text, and distribution lists that exceed 2 KB. Items of this size are stored more efficiently as files than as database records. The message database contains a pointer to where each item is found.

Guardian Database

The guardian database (`ngwguard.db`) serves as the master copy of the data dictionary information for the following subordinate databases in the post office:

- User databases (user*xxx*.db)
- Message databases (msg*nnn*.db)
- Prime user databases (pu*xxxxx*.db)
- Library databases (`dmsh.db` and dm*xxnn01-FF*.db)

The guardian database is vital to GroupWise functioning. Therefore, the POA has an automated fall-back and roll-forward process to protect it. The POA keeps a known good copy of the guardian database called `ngwguard.fbk`. Whenever it modifies the `ngwguard.db` file, the POA also records the transaction in the roll-forward transaction log called `ngwguard.rfl`. If the POA detects damage to the `ngwguard.db` file on startup or during a write transaction, it goes back to the `ngwguard.fbk` file (the "fall back" copy) and applies the transactions recorded in the `ngwguard.rfl` file to create a new, valid and up-to-date `ngwguard.db`.

In addition to the POA fall-back and roll-forward process, you should still back up the `ngwguard.db`, `ngwguard.fbk`, and `ngwguard.rfl` files regularly to protect against media failure. Without a valid ngwguard.db file, you cannot access your email. With current `ngwguard.fbk` and `ngwguard.rfl` files, a valid `ngwguard.db` file can be rebuilt should the need arise.

The ngwguard.dc file is the structural template for building the guardian database and its subordinate databases. Also called a dictionary file, the ngwguard.dc file contains schema information, such as data types and record indexes. If this dictionary file is missing, no additional databases can be created in the post office.

Agent Input/Output Queues in the Post Office

Each post office contains agent input/output queues where messages are deposited and picked up for processing by the POA and the MTA. The MTA transfers messages into and out of the post office, while the POA handles message delivery.

MTA Output Queue in the Post Office

The MTA output queue in each post office is the *post_office*\wpcsout folder.

The MTA typically has a TCP/IP link to the post office. The MTA transfers user messages to the POA by way of TCP/IP. The POA then stores the messages in the MTA output queue on behalf of the MTA, so the MTA does not need write access to the post office.

The *post_office*\wpcsout\ofs subfolder is where the MTA transfers user messages for delivery by the POA to users' mailboxes in the local post office.

The MTA *post_office*\wpcsout\ads subfolder is where the MTA transfers administrative messages instructing the POA admin thread to update the post office database (wphost.db).

POA Input Queue in the Post Office

The POA input queue in each post office is the *post_office*\wpcsout folder, which is the same as the MTA output queue.

The *post_office*\wpcsout\ofs subfolder is where the POA picks up user messages deposited there by the MTA and updates the local message store, so users receive their messages.

The *post_office*\wpcsout\ads subfolder is where the POA admin thread picks up administrative messages deposited there by the MTA and updates the post office database (wphost.db).

POA Output Queue in the Post Office

The POA output queue (*post_office*\wpcsin) is where the POA deposits user messages for the MTA to transfer to other domains and post offices.

MTA Input Queue in the Post Office

The MTA input queue in each post office (*post_office*\wpcsin) is the same as the POA output queue. The MTA picks up user messages deposited there by the POA and transfers them to other domains and post offices.

Libraries (optional)

A library is a collection of documents and document properties stored in a database system that can be managed and searched. You do not need to set up libraries unless you are using GroupWise Document Management Services (DMS). See Part XIII, "Libraries and Documents," on page 511.

Library Databases

The databases for managing libraries are stored in the `gwdms` folder and its subfolders in the post office.

The `dmsh.db` file is a database shared by all libraries in the post office. It contains information about where each library in the post office is located.

Each library has its own subfolder in the `gwdms` folder. In each library folder, the `dm`*`xxnn`*`01-`*`FF`*`.db` files contain information specific to that library, such as document properties and what users have rights to access the library.

Document Storage Areas

The actual documents in a library are not kept in the library databases. They are kept in a document storage area, which consists of a series of folders for storing document files. Documents are encrypted and stored in BLOBs (binary large objects) to make document management easier. A document, its versions, and related objects are stored together in the same BLOB.

A document storage area might be located in the post office folder structure, or in some other location where more storage space is available. If it is located in the post office, the document storage area can never be moved. Therefore, storing documents in the post office folder structure is not usually recommended. If it is stored outside the post office, a document storage area can be moved when additional disk space is required.

Role of the Post Office Agent

The GroupWise Post Office Agent (POA) delivers messages to users' mailboxes, connects users to their post offices in Online mode, updates post office databases, indexes messages and documents, and performs other post office-related tasks.

The following sections help you understand the various functions of the POA:

Client/Server Processing

Using client/server access mode, the GroupWise client maintains one or more TCP/IP connections with the POA and does not access the post office directly. Consequently, the performance of the POA in responding to requests from the GroupWise client directly affects the GroupWise client's responsiveness to users.

When using client/server access mode, the GroupWise client can be configured to control how much time it spends actually connected to the POA.

- In Online mode, the client is continuously connected.
- In Caching mode, the client connects at regular intervals to check for incoming messages and also whenever the client user sends a message. Address lookup is performed locally. Caching mode allows the POA to service a much higher number of users than Online Mode.
- In Remote mode, the client connects whenever the client user chooses, such as when using a brief modem connection to download and upload messages.

For more information about the client modes available with client/server access mode, see "Using Caching Mode" and "Using Remote Mode" in the *GroupWise 18 Client User Guide*

Client/server access mode also allows users to access their GroupWise mailboxes from POP and IMAP clients, in addition to the GroupWise client. See “Supporting IMAP Clients” on page 147.

In client/server access mode, the POA is enabled for secure SSL connections by default. If necessary, you can configure the POA to force SSL connections with all clients. See “Securing the Post Office with SSL Connections to the POA” on page 152.

Message File Processing

Messages from users in other post offices arrive in the local post office in the form of message files deposited in the POA input queue. See “Agent Input/Output Queues in the Post Office” on page 138.

The POA picks up the message files and updates all user and message databases to deliver incoming messages in the local post office. To provide timely delivery for a large volume of incoming messages, see “Optimizing Message File Processing” on page 173.

Other POA Functions

In addition to client/server processing (interacting with client users) and message file processing (delivering messages), the POA:

- Performs indexing tasks.

  See “Configuring Indexing” on page 177.
- Performs scheduled maintenance on databases in the post office.

  See “Scheduling Database Maintenance” on page 154.
- Monitors and manages disk space usage in the post office.

  See “Scheduling Disk Space Management” on page 156.
- Restricts the size of messages that users can send outside the post office.

  See “Restricting Message Size between Post Offices” on page 149.
- Primes users’ mailboxes for Caching mode.

  See “Supporting Forced Mailbox Caching” on page 149.
- Performs nightly user upkeep so users do not need to wait while the GroupWise client performs it; also creates a downloadable version of the GroupWise Address Book for Remote and Caching users.

  See “Configuring Nightly User Upkeep” on page 157.
- Provides LDAP authentication.

  See “Providing LDAP Authentication for GroupWise Users” on page 153.
- Provides LDAP server pooling.

  See “Configuring a Pool of LDAP Servers” on page 83
- Prevents unauthorized access to the post office.

  See “Configuring Intruder Detection” on page 153.
- Tracks the GroupWise client software in use in the post office.

  See “Checking What GroupWise Clients Are in Use” on page 148.
- Automatically detects and repairs invalid information in user databases (`user`*`xxx`*`.db`) and message databases (`msg`*`nnn`*`.db`) for the local post office by using an efficient multi-threaded process.

  See “Optimizing Database Maintenance” on page 174.

* Automatically detects and repairs invalid information in the post office database (`wphost.db`).
* Automatically detects and repairs damage to the guardian database (`ngwguard.db`) in the post office.
* Updates the post office database whenever GroupWise users, resources, post offices, or other GroupWise objects are added, modified, or deleted.
* Replicates shared folders between post offices.
* Executes GroupWise client rules.
* Processes requests from GroupWise Remote users.

15 Configuring the POA

For POA system requirements, see "Hardware and Operating System Requirements" in the *GroupWise 18 Installation Guide*. The POA is automatically installed and started when you create a new post office.

As your GroupWise system grows and evolves, you might need to modify POA configuration to meet the changing needs of the post office it services. The following topics help you configure the POA:

- "Performing Basic POA Configuration" on page 143
  - Configuring the POA in the GroupWise Admin Console
  - Binding the POA to a Specific IP Address
  - Configuring the POA for Remote Server Login (Windows Only)
- "Configuring User Access to the Post Office" on page 145
  - Simplifying Client Access with a GroupWise Name Server
  - Supporting IMAP Clients
  - Supporting SOAP Clients
  - Checking What GroupWise Clients Are in Use
  - Supporting Forced Mailbox Caching
  - Restricting Message Size between Post Offices
  - Supporting Calendar Publishing
- "Configuring Post Office Security" on page 150
  - Securing Client Access through an External Proxy Server
  - Controlling Client Redirection Inside and Outside Your Firewall
  - Securing the Post Office with SSL Connections to the POA
  - Providing LDAP Authentication for GroupWise Users
  - Configuring Intruder Detection
  - Configuring Trusted Application Support
- "Configuring Post Office Maintenance" on page 154
  - Scheduling Database Maintenance
  - Scheduling Disk Space Management
  - Configuring Nightly User Upkeep

Performing Basic POA Configuration

POA configuration information is stored as properties of its POA object in the internal GroupWise directory. The following topics help you to modify the POA object in the GroupWise Admin console and to change POA configuration to meet changing system configurations:

Creating a New POA in the GroupWise Admin Console

The initial POA object is automatically created when you create a new post office. Typically, you do not need more than one POA in a post office, but it you want to customize the processing of multiple POAs, you can do so. When you create the new POA object, the GroupWise Admin Service configures and starts the new POA.

For an example of why you might need to create a second POA object, see "Controlling Client Redirection Inside and Outside Your Firewall" on page 151.

1. In the GroupWise Admin console, click **Post Office Agents > New**.
2. Specify a unique name for the new POA object.
3. Select the post office that you are creating a new POA object for.
4. Specify the IP address or DNS hostname of the post office server.
5. (Conditional) If more than one POA will run on the same server, use new unique port numbers for the new POA.
6. (Conditional) If the new POA will run on a remote server:
   - **6a** Install the GroupWise Server component on the remote server.
   - **6b** Create the POA service:

     ```
     gwadminutil services -i /path_to_post_office -n poa_name
     ```
   - **6c** Create the certificate for the POA server:

     ```
     gwadminutil certinst -db /path_to_post_office -n poa_name
                          -ca domain_ip_address:9710 -a admin_user -p
     ```
   - **6d** Restart the GroupWise Admin Service.
   - **6e** Start the POA.

Configuring the POA in the GroupWise Admin Console

The advantage to configuring the POA in the GroupWise Admin console, as opposed to using startup switches in a POA startup file, is that the POA configuration settings can be easily edited from any location where the Admin console is available.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the tabs to configure each aspect of the POA.
3. For information about each tab and field, click **Help**.

   Many of the fields on POA object tabs correspond to POA startup switches. Some POA configuration can be done only using startup switches. For more information, see Chapter 20, "Using POA Startup Switches," on page 183.

Binding the POA to a Specific IP Address

You can cause the POA to bind to a specified IP address when the server where it runs uses multiple IP addresses. The specified IP address is associated with all ports used by the agent. Without an exclusive bind, the POA binds to all IP addresses available on the server.

IMPORTANT: If you bind the POA (or MTA) to a specific IP address, the Admin Service is also bound to that IP address.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Agent Settings** tab.
3. Select **Bind Exclusively to TCP/IP Address**.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --ip and --mtpoutport startup switch in the POA startup file to establish an exclusive bind to the specified IP address.

Configuring the POA for Remote Server Login (Windows Only)

On Windows, you can organize a post office so that some components, such as a library, remote document storage area, or restore area are located on a remote Windows server. In order for the POA access the remote Windows server, you must provide a user name and password that provide sufficient access to the remote server for the POA to perform the required task on the remote server.

1. In the GroupWise Admin console, browse to and click the name of the post office that includes remote components.
2. Click the **Settings** tab.
3. In the **Remote File Server Settings** section, provide the user name and password that the POA can use to log in to the remote Windows server where post office components are located.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Configuring User Access to the Post Office

The GroupWise client uses client/server access to the post office. The following topics help you configure the POA to customize the types of client/server access provided to the post office:

Simplifying Client Access with a GroupWise Name Server

A GroupWise name server redirects each GroupWise client user to the IP address and port number of the POA that services the user's post office. By setting up a GroupWise name server, GroupWise client users do not need to know and provide any IP address information when they start the GroupWise client. The GroupWise name server takes care of this for them.

- "Required Hostnames" on page 145
- "Required Port Number" on page 146
- "How a GroupWise Name Server Helps the GroupWise Client Start" on page 146
- "Setting Up a GroupWise Name Server" on page 146

Required Hostnames

The primary GroupWise name server must be designated using the hostname `ngwnameserver`. You can also designate a backup GroupWise name server using the hostname `ngwnameserver2`.

Required Port Number

Each server designated as a GroupWise name server must have a POA running on it that uses the default port number of 1677. Other agents can run on the same server, but one POA must use the default port number of 1677 in order for the GroupWise name server to function.

How a GroupWise Name Server Helps the GroupWise Client Start

After a server has been designated as `ngwnameserver`, and a POA using the default port number of 1677 is running on that server, the GroupWise client can connect to the POA of the appropriate post office by contacting the POA located on `ngwnameserver`. If `ngwnameserver` is not available, the client next attempts to contact the backup name server, ngwnameserver2. If no GroupWise name server is available, the user must provide the IP address and port number of the appropriate POA in order to start the GroupWise client in client/server mode.

Setting Up a GroupWise Name Server

1. Ensure that TCP/IP is set up and functioning on your network.
2. Know the IP address of the server you want to set up as a GroupWise name server.
3. Ensure that the POA on that server uses the default TCP port of 1677.
4. If you want a backup GroupWise name server, identify the IP address of a second server where the POA uses the default TCP port of 1677.
5. Use your tool of choice for modifying DNS.

Linux:	You can use the YaST Control Center.
Windows:	You can use DNS Manager.

6. Create an entry for the IP address of the first POA and give it the hostname `ngwnameserver`.
7. If you want a backup name server, create an entry for the IP address of the second POA and give it the hostname `ngwnameserver2`.

   You must use the hostnames `ngwnameserver` and `ngwnameserver2`. Any other hostnames are not recognized as GroupWise name servers.
8. Save your changes.

As soon as the hostname information replicates throughout your system, GroupWise client users can start the GroupWise client without specifying a TCP/IP address and port number.

Supporting IMAP Clients

Internet Messaging Application Protocol (IMAP) is used by email clients such as Microsoft Outlook and Evolution. You can configure the POA to communicate with IMAP-enabled email clients much like the GroupWise client does.

NOTE: IMAP clients connecting to your GroupWise system from outside your firewall must connect through the GWIA, rather than through the POA. Connecting directly through the POA provides faster access for internal IMAP clients. For more information, see Section 31, "Configuring POP3/IMAP4 Services," on page 307.

---

1 In the GroupWise Admin console, browse to and click the POA.

2 Click the **Agent Settings** tab.

3 Fill in the following fields:

   Enable IMAP: Select **Enable IMAP** to turn on IMAP processing.

   Max IMAP Threads: Specify the maximum number of IMAP threads you want to the POA to start.

   The default maximum number of IMAP threads is 40. This is adequate for most post offices, because each IMAP thread can service multiple IMAP clients. By default, the POA creates 2 IMAP threads and automatically creates additional threads as needed to service clients until the maximum number is reached. You cannot set the maximum higher than 40.

   You might want to lower the maximum number of IMAP threads if IMAP processing is monopolizing system resources that you prefer to have available for other processes. However, insufficient IMAP threads can cause slow response for IMAP client users.

   Port: Use the default port of 143 unless it is already in use on the server.

   SSL: Select from the following options to configure this POA's use of secure connections to IMAP clients. In order to use an SSL connection, the IMAP clients must also be enabled for SSL.

   - **Disabled:** The POA does not support SSL connections.
   - **Enabled:** The POA uses SSL if both the POA and the IMAP client can handle SSL. If either side cannot handle SSL, the IMAP connection is still accepted. An SSL-enabled POA accepts non-SSL connections on port 143 and SSL connections on port 993.
   - **Required:** The POA uses SSL if both the POA and the IMAP client can handle SSL. If either side cannot handle SSL, the IMAP connection is still accepted. An SSL-enabled POA accepts non-SSL connections on port 143 and SSL connections on port 993.

4 Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --imap, --imapmaxthreads, --imapport, --imapssl, and --imapsslport startup switches in the POA startup file to configure the POA to support IMAP clients. In addition, you can use the --imapreadlimit and --imapreadnew startup switches to configure how the POA downloads messages to IMAP clients.

POA Console: You can see whether IMAP is enabled on the Configuration page under the **General Settings** heading.

Supporting SOAP Clients

Simple Object Access Protocol (SOAP) is used by email clients such as Evolution and other clients such as GroupWise WebAccess and the GroupWise Mobility Service to access mailboxes. You can configure the POA to communicate with SOAP-enabled email clients much like the GroupWise client does. Starting in GroupWise 18, SOAP is enabled by default.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Agent Settings** tab.
3. Fill in the following fields:

   Enable SOAP: Select **Enable SOAP** to turn on SOAP processing.

   Max SOAP Threads: Specify the maximum number of SOAP threads you want the POA to start.

   The default maximum number of SOAP threads is 40. This is adequate for most post offices, because each SOAP thread can service multiple SOAP clients. By default, the POA creates 4 SOAP threads and automatically creates additional threads as needed to service clients until the maximum number is reached. You cannot set the maximum higher than 40.

   You might want to lower the maximum number of SOAP threads if SOAP processing is monopolizing system resources that you prefer to have available for other processes. However, insufficient SOAP threads can cause slow response for SOAP client users.

   Port: Use the default port of 7191 unless it is already in use on the server.

   SSL: Select from the following options to configure this POA's use of secure connections to SOAP clients. In order to use an SSL connection, the SOAP clients must also be enabled for SSL.

   - **Disabled:** The POA does not support SSL connections.
   - **Required:** The POA uses SSL if both the POA and the SOAP client can handle SSL.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --soap, --soapmaxthreads, --soapport, --soapssl, and --soapthreads startup switches in the POA startup file to configure the POA to support SOAP clients. In addition, you can use the --evocontrol startup switch to configure the POA to allow only specified versions of Evolution to connect to the post office.

POA Console: You can see whether SOAP is enabled on the Configuration page under the **General Settings** heading.

Checking What GroupWise Clients Are in Use

You can configure the POA to identify GroupWise client users who are running GroupWise clients that do not correspond to a specified release version and/or date. You can also force them to update to the specified version. For setup instructions, see “Restricting Client Access to the Post Office” on page 129.

Corresponding Startup Switches: You can also use the --gwclientreleaseversion, --gwclientreleasedate, and --enforceclientversion startup switches in the POA startup file to configure the POA to check client version and/or date information.

POA Console: On the Status page of the POA console, click **C/S Users** to display the Current Users page, which lists all GroupWise users who are currently accessing the post office. Users who are running GroupWise clients older than the approved version and/or date are highlighted in red in the list. Users who are running newer versions are shown in blue.

If the POA console is password protected as described in "Configuring the POA Console" on page 159, you can change the expected release dates for the current POA session. Under **Client/ Server Settings**, click **Enforce Lockout on Older GroupWise Clients**.

Supporting Forced Mailbox Caching

GroupWise client users have the option to download their GroupWise mailboxes to their workstations so they can work without being continuously connected to the network. This is called Caching mode. For more information, see "Caching Mode" on page 539.

When client users change to Caching mode, the contents of their mailboxes must be copied to their hard drives. This process is called "priming" the mailbox. If users individually decide to use Caching mode, the POA easily handles the process.

If you force all users in the post office to start using Caching mode, as described in "Allowing or Forcing Use of Caching Mode" on page 540, multiple users might attempt to prime their mailboxes at the same time. This creates a load on the POA that can cause unacceptable response time for other users.

To configure the POA to handle multiple requests to prime mailboxes:

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Agent Settings** tab.
3. Set **Max Thread Usage for Priming and Moves** as needed.

   By default, the POA allocates 30% of its client/server handler threads for priming mailboxes for users who are using Caching mode for the first time. By default, the POA starts 10 client/server handler threads, so in a default configuration, three threads are available for priming. You might want to specify 60 or 80 so that 60% to 80% of POA threads are used for priming mailboxes. You might also want to increase the number of client/server handler threads the POA can start in order to handle the temporarily heavy load while users are priming their mailboxes. See "Adjusting the Number of Client/Server Connections" on page 172.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --primingmax switch in the POA startup file to configure the POA to handle multiple requests to prime mailboxes.

POA Console: If the POA console is password protected as described in "Configuring the POA Console" on page 159, you can change the POA's ability to respond to caching requests for the current POA session on the Configuration page. Under the **Client/Server Settings** heading, click **Max Thread Usage for Priming and Live Moves**. To increase the number of client/server threads, click **Client/Server Processing Threads** under the **Performance Settings** heading.

Restricting Message Size between Post Offices

You can configure the POA to restrict the size of messages that users are permitted to send outside the post office.

1. In the GroupWise Admin console, browse to and click the name of a domain.
2. Click **Post Office Links**, then click the name of the post office.
3. In the **Maximum Send Message Size** field, specify in megabytes the size of the largest message you want users to be able to send outside the post office, then click **OK**.

   A setting of 0 (zero) indicates that no size limitations have been set.

If a user's message is not sent out of the post office because of this restriction, the user receives an email notification message with a subject line of:

```
Delivery disallowed
```

The notification message also includes the subject of the original message. This message provides information to the user about why and where the message was disallowed. However, the message is still delivered to recipients in the sender's own post office.

There are additional ways to restrict the size of messages that users can send, as described in "Restricting the Size of Messages That Users Can Send" on page 125.

Corresponding Startup Switches: You can also use the --mtpsendmax startup switch in the POA startup file to restrict message size.

POA Console: You can view the maximum message size on the Configuration page. If the POA console is password protected as described in "Configuring the POA Console" on page 159, you can change the maximum message size for the current POA session using the **Message Transfer Protocol** link on the Configuration page.

Supporting Calendar Publishing

See "Configuring a POA for Calendar Publishing" in the *GroupWise 18 Installation Guide*.

Configuring Post Office Security

You can configure the POA in various ways to meet the security needs of the post office.

Securing Client Access through an External Proxy Server

If the server where the POA runs is behind your firewall, you can link it to an external proxy server in order to provide client/server access to the post office for GroupWise client users who are outside the firewall. You could also use generic proxy, network address translation (NAT), and port address translation (PAT) to achieve the same results.

If the POA is configured with both an internal IP address and an external proxy IP address, the POA returns both IP addresses to the GroupWise client when it attempts to log in. The client tries the internal address first, and if that does not succeed, it tries the external proxy address, then it records which address succeeded. If the user moves from inside the firewall to outside the firewall, the client might fail to log in on the first attempt, but succeeds on the second attempt.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Agent Settings** tab, and find the **Network Address** section.
3. In the **External IP Address** field in the **Network Address** section, specify the external IP address of the external server that GroupWise client users access from outside your firewall.

   Typically, this is the public IP address presented by your external proxy server, generic proxy, NAT, or PAT.
4. (Conditional) If you want to use a different port number for the external proxy server than you are using for client/server access to the POA itself, provide the port number in the **External Port** field in the Client/Server section.

The network router is responsible for enabling the Network Address Translation (NAT) or Port Address Translation (PAT) between the external client requests and the internal network address of the POA. The external proxy server address and port should be listed as they are seen from the external GroupWise clients. The POA provides this address and port to clients that attempt to connect from outside the firewall.

If you are using NAT, provide an external server IP address for the POA, and in the **Port** field, use port 1677 (the default) for the external client/server port. If you are using PAT, provide an external server IP address for the POA, and in the **Port** field, use a unique external client/server port.

5 Click **Save**, then click **Close** to return to the main Admin console window.

POA Console You can list all POAs in your GroupWise system, along with their external IP addresses. On the Configuration page, click **IP Addresses Redirection Table** under the **General Settings** heading.

Controlling Client Redirection Inside and Outside Your Firewall

When a user tries to access his or her mailbox without providing the IP address of the POA for his or her post office, any POA or a GroupWise name server POA can redirect the request to the POA for the user's post office.

A POA that is configured with both an internal IP address and an external IP address automatically redirects internal users to internal IP addresses and external users to external IP addresses. However, if you want to control which users are redirected to which IP addresses based on criteria other than user location, you can configure a post office with one POA to always redirect users to internal IP addresses and a second POA to always redirect users to external IP addresses. Users are then redirected based on which POA IP address they provide in the GroupWise Startup dialog box when they start the GroupWise client to access their mailboxes.

1 Configure the initial POA for the post office with the IP address that you want for internal users.

Do not fill in the **External IP Address** field on the **Agent Settings** tab of the POA object.

2 Create a second POA object in the post office and give it a unique name, such as POA_EXT.

For instructions, see "Creating a New POA in the GroupWise Admin Console" on page 144.

3 Configure this second POA with an external IP address.

For instructions, see "Securing Client Access through an External Proxy Server" on page 150.

Do not fill in the **TCP/IP Address** field on the **Agent Settings** tab of the POA object.

4 Start the new instance of the POA.

5 Give users that you want to be redirected to internal IP addresses the IP address you used in Step 1.

6 Give users that you want to be redirected to external IP addresses the IP address you used in Step 3.

Securing the Post Office with SSL Connections to the POA

Secure Sockets Layer (SSL) ensures secure communication between the POA and other programs by encrypting the complete communication flow between the programs. By default, the POA is enabled to use SSL connections, but SSL connections are not required.

For background information about SSL and how to set it up on your system, see “Server Certificates and SSL Encryption” on page 695.

To configure the POA to require SSL:

1 In the GroupWise Admin console, browse to and click the POA.

2 Click the **SSL Settings** tab.

3 (Conditional) If you need to generate a new self-signed certificate for the POA:

   The GroupWise Admin Service generates a certificate signing request (CSR) and a private key file, and then sends them to the GroupWise certificate authority (CA) on the primary domain. The CA issues the requested certificate, which is then returned to the local server.

   3a Click **Generate Certificate**.

   3b Specify and confirm the password for the private key file for the new SSL certificate, then click **OK**.

   The newly created SSL certificate and private key files display on the **SSL Settings** tab.

   3c Click **Save** to save the SSL certificate and key files.

4 (Conditional) If you already have an SSL certificate and key file for the POA:

   4a In the **SSL Certificate File** field, click the **Browse** icon.

   4b Click **Upload Local File to Server**, then click **Browse**.

   4c Browse to and select the SSL certificate file on your local workstation.

   You can use certificate files in the PEM, PFX, CRT, B64, or CER format.

   4d Click **Upload** to upload the certificate file into the GroupWise `certificates` folder on the server where the POA is running.

   4e Click **OK**.

   4f In the **SSL Key File** field, browse to, select, and upload the private key file, then click **OK**.

   4g Click **Save** to save the SSL certificate and key files.

5 To enable or require SSL connections with the MTA, with GroupWise clients, and with other programs that communicate with the POA, click the **Agent Settings** tab.

6 To enable or require SSL connections between the POA and its MTA, select **Enabled** or **Required** in the **Message Transfer SSL** drop-down list.

   The MTA must also use SSL for the connection to be secure. See “Securing the Domain with SSL Connections to the MTA” on page 229.

   IMPORTANT: To prevent closed links between agents, select **Enabled** when you are initially configuring agents for SSL. Select **Required** for tighter security only after all agents are successfully using SSL.

   ---

7 To enable or require SSL for other protocols, scroll down the **Agent Settings** tab to the **SSL** fields and select the desired SSL settings.

8 Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --certfile, --keyfile, --keypassword, --httpssl, --mtpssl, --imapssl, and --imapsslport switches in the POA startup file to configure the POA to use SSL.

POA Console: You can view SSL information for the POA on the Status and Configuration pages. In addition, when you list the client/server users that are accessing the post office, SSL information is displayed for each user.

Providing LDAP Authentication for GroupWise Users

By default, GroupWise client users' passwords are stored in GroupWise user databases, and the POA authenticates users to their GroupWise mailboxes by using those GroupWise passwords. For background information about passwords, see Chapter 89, "GroupWise Passwords," on page 687.

By enabling LDAP authentication for the POA, users' password information can be retrieved from an LDAP directory such as NetIQ eDirectory and Microsoft Active Directory. For background information about LDAP, see "Authenticating to GroupWise with Passwords Stored in an LDAP Directory" on page 699.

When you enable LDAP authentication, it is important to provide fast, reliable access to the LDAP directory because GroupWise client users cannot access their mailboxes until they have been authenticated.

1 Set up an LDAP directory for use with GroupWise.

   For instructions, see "Setting Up an LDAP Directory" on page 79.

2 Set up at least one LDAP server for use with the LDAP directory.

   For instructions, see "Setting Up an LDAP Server" on page 81.

3 Click **Post Offices**, click the name of a post office where you want to provide LDAP authentication for GroupWise users, then click the **Security** tab.

4 Select **LDAP Authentication**.

5 Move at least one LDAP server from the **Available LDAP Servers** list to the **Selected LDAP Servers** list.

   For more information, see "Configuring a Pool of LDAP Servers" on page 83.

6 Click **Save**, then click **Close** to return to the main Admin console window.

Configuring Intruder Detection

By default, the POA is configured to detect system break-in attempts in the form of repeated unsuccessful logins. You can customize how the POA recognizes and responds to break-in attempts.

1 In the GroupWise Admin console, browse to and click the name of the post office.

2 Click the **Client Settings** tab.

3 Specify how many unsuccessful login attempts are allowed before the user is locked out.

   The default is 5; valid values range from 3 to 10.

4 Specify in minutes how long unsuccessful login attempts are counted.

   The default is 15; valid values range from 15 to 60.

5 Specify in minutes how long the user login is disabled.

   The default is 30; the minimum setting is 15.

6 Click **Save**, then click **Close** to return to the main Admin console window.

If a user is locked out by intruder detection, his or her GroupWise account is disabled. To restore access, follow the instructions in "Unlocking GroupWise Accounts" on page 473.

Corresponding Startup Switches: You can also use the --intruderlockout, --incorrectloginattempts, --attemptsresetinterval, and --lockoutresetinterval startup switches in the POA startup file to configure the POA for intruder detection.

POA Console: You can view current intruder detection settings on the Configuration page. If the POA console is password protected as described in "Configuring the POA Console" on page 159, you can change the settings by clicking the **Intruder Detection** link. You cannot disable intruder detection from the POA console.

Configuring Trusted Application Support

Trusted applications are third-party programs that can log into POAs and GWIAs in order to access GroupWise mailboxes without needing personal user passwords. Trusted applications might perform such services as message retention or synchronization with mobile devices.

For background information about setting up trusted applications, see "Trusted Applications" on page 64.

Configuring Post Office Maintenance

You can configure the POA to manage databases and disk space in the post office on a regular basis:

Scheduling Database Maintenance

By default, the POA performs the following database maintenance events:

- **Default Daily Maintenance Event:** The default daily maintenance event occurs at 2:00 a.m. The POA performs a Structure check on user, message, and document databases and fixes any problems it encounters.
- **Default Weekly Maintenance Event:** The default weekly maintenance event occurs on Saturday at 3:00 a.m. The POA runs and Audit Report and a Content check. The Audit report lists the type of license (full vs. limited) each mailbox requires and which mailboxes haven't been accessed for at least 60 days. The Content check verifies pointers from user databases to messages in message databases and pointers from message databases to attachments in the `offiles` folder structure, and fixes any problems it encounters.

You can modify the default database maintenance events, or create additional database maintenance events for the POA to perform on a regular basis.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Scheduled Events** tab.

   The Scheduled Events tab lists a pool of POA events available to all POAs in your GroupWise system.
3. To modify the default daily database maintenance event, which affects all POAs that have this database maintenance event enabled, select **Default Daily Maintenance Event**, then click **Edit**.

   or

   To modify the default weekly database maintenance event, which affects all POAs that have this database maintenance event enabled, select **Default Weekly Maintenance Event**, then click **Edit**.

or

To create a new database maintenance event, which is added to the pool of POA events that can be enabled for any POA in your GroupWise system, click **New**, then type a name for the new database maintenance event. Select **Mailbox/Library Maintenance** in the **Type** field.

4 In the **Trigger** section, specify when you want the database maintenance event to take place.

You can have the database maintenance event take place once a week, once a day, or at any other regular interval, at whatever time you choose.

The list below the **Trigger** box displays the pool of POA database maintenance actions that are available for inclusion in all POA database maintenance events in your GroupWise system.

5 To modify a default database maintenance action, select one of the existing actions, then click **Edit**.

or

To create a new database maintenance action, click **New**, then type a name for the new database maintenance action.

Database maintenance actions and options you can schedule include:

Actions	Options on Actions
Analyze/Fix Databases	**Databases**
Structure Index check Contents Collect statistics Attachment file check Fix problems Update user disk space totals	User Message Document **Logging** Log file Verbose log level
Analyze/Fix Library	**Results mailed to**
Verify library Fix document/version/element Verify document files Validate all document security Synchronize user name Remove deleted storage areas Reassign orphaned documents Reset word lists	Administrator Individual users **Misc** Support options **Exclude** Selected users

For more detailed descriptions of the actions, click **Help** in the Scheduled Event Actions dialog box. See also:

- Chapter 43, “Maintaining User/Resource and Message Databases,” on page 403
- Chapter 44, “Maintaining Library Databases and Documents,” on page 407

6 Select and configure the database maintenance action to perform for the database maintenance event., then click **OK** to return to the **Scheduled Events** tab.

7 Click **Save**, then click **Close** to return to the main Admin console window.

POA Console You can see what database maintenance events the POA is scheduled to perform at the bottom of the Configuration page.

Scheduling Disk Space Management

By default, the POA performs one recurring disk space management event. Every 5 minutes, the POA checks to ensure there is at least 2048 MB of free disk space in the post office folder. If there is less than 2048 MB of free disk space, the POA performs a Reduce operation on the user and message databases in the post office. If available disk space drops below 200 MB, the POA stops processing mail.

You can modify this default disk space management event, or create additional disk space management events for the POA to perform on a regular basis.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Maintenance** tab.
3. To change the interval at which the POA checks for free disk space in its post office, adjust the number of minutes in the **Disk Check Interval** field as needed.

   The default is 5 minutes, which could be much too frequent if ample disk space is readily available.

   When a disk space problem is encountered, the time interval no longer applies until after the situation has been corrected. Instead, the POA continually checks available disk space to determine if it can restart message threads that have been suspended because of the low disk space condition.
4. To change the amount of time the POA allows to pass before notifying the administrator again about a problem condition that has already been reported, adjust the number of hours in the **Disk Check Delay** field as needed.

   The default is 2 hours.
5. Click **Save**.
6. Click the **Scheduled Events** tab.

   The Scheduled Events tab lists a pool of POA events available to all POAs in your GroupWise system.
7. To modify the default disk space management event, which affects all POAs that have this disk space management event enabled, select **Default Disk Check Event**.

   or

   To create a new disk space management event, which is added to the pool of POA events that can be enabled for any POA in your GroupWise system, click **New**, then type a name for the new disk space management event. Select **Disk Check** in the **Type** field.
8. In the **Trigger** box, select **Percent** or **MB** to determine whether you want the amount of available disk space measured by percentage or by megabytes.
9. In the **Trigger Action At** field, specify the minimum amount of available disk space you want to have in the post office. When the minimum amount is reached, the Disk Check actions are triggered
10. In the **Stop Mail Processing At** field, specify the minimum amount of available disk space at which you want the POA to stop receiving and processing messages.

    The list below the **Trigger** box displays the pool of disk space management actions that are available for inclusion in all POA disk space management events in your GroupWise system.
11. To modify the action that the default disk space management event includes, select **Default Disk Space Management Actions**.

    or

To create a new disk space management action, click **New**, then type a name for the new disk space management action.

Disk space management actions and options you can schedule include:

Actions	Options on Actions
Expire/Reduce Messages	**Databases**
Reduce only	User
Expire and reduce	Message
- Items older than	**Logging**
- Downloaded items older than	Log file
- Items larger than	Verbose log level
- Trash older than	**Results mailed to**
- Reduce mailbox to	Administrator
- Reduce mailbox to limited size	Individual users
Include	**Misc**
- Received items	Support options
- Sent items	**Exclude**
- Calendar items	Selected users
- Only backed-up items	**Notification**
- Only retained items	Notify administrator when action begins
Archive/Delete Documents	Notify administrator if action fails
Delete Activity Logs	Notify administrator when action completes

For more detailed descriptions of the actions, click **Help** in the Scheduled Event Actions dialog box. See also Chapter 46, "Managing Database Disk Space," on page 413.

12 Select and configure the disk space management action to perform.

13 Click OK to return to the **Scheduled Events** tab.

14 Click **Save**, then click **Close** to return to the main Admin console window.

You might want to create several disk space management events with different triggers and actions. For some specific suggestions on implementing disk space management, see "Managing Disk Space Usage in the Post Office" on page 121.

POA Console You can view the currently scheduled disk check events on the Scheduled Events page.

Configuring Nightly User Upkeep

By default, the POA performs the following activities each day to keep GroupWise users' mailboxes and calendars up-to-date:

- Advance uncompleted tasks to the next day
- Delete expired items from users' mailboxes
- Empty expired items from the Trash

* Synchronize each user's Frequent Contacts Address Book and personal address books with the GroupWise Address Book
* Synchronize user addresses in personal groups with the GroupWise Address Book, in case users have been moved, renamed, or deleted

The upkeep performed is determined by the settings located in each user's Cleanup options (User object > **Client Options > Environment Options > Cleanup**). Auto-Delete is run by the POA during user upkeep, but Auto-Archive is run by the client as soon as the user accesses his or her mailbox. In Caching mode, Auto-Delete is also run by the client.

Unread items such as messages and upcoming appointments are not deleted. However, unread calendar items such as appointments, reminder notes, and tasks that are scheduled in the past are deleted.

Although user upkeep includes deletion activities, it does not necessarily reduce mailbox disk space usage. To reduce disk space usage, see "Managing Disk Space Usage in the Post Office" on page 121.

Synchronization of personal address books with the GroupWise Address Book enables the latest contact information to be synchronized to users' mobile devices when a synchronization solution such as GroupWise Mobility Service has been implemented. When users copy contacts from the GroupWise Address Book to personal address books, changes made in the GroupWise Address Book are mirrored in personal address books and, therefore, are available for synchronization to mobile devices. However, changes to copied contacts made on mobile devices are not retained in GroupWise because the contact information from the GroupWise Address Book always overrides the contact information of the copied contacts.

You can change the time of day when the POA takes care of these user upkeep activities.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Maintenance** tab.
3. In the **Start User Upkeep** field, specify the number of hours after midnight for the POA to start performing user upkeep.

   The default is 1 hour.
4. If you have Remote or Caching users, specify the number of hours after midnight for the POA to generate the daily copy of the GroupWise Address Book for Remote and Caching users.

   The default is 0 hours (that is, at midnight).

   If you want to generate the GroupWise Address Book for download more often than once a day, you can delete the existing `wprof50.db` file from the `\wpcsout\ofs` subfolder of the post office. A new downloadable GroupWise Address Book is automatically generated for users in the post office.

   In addition to this feature, the POA automatically tracks changes to the GroupWise Address Book and provides automatic synchronization.

   For more information, see "Controlling Address Book Synchronization for Caching and Remote Client Users" on page 75.
5. Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also configure nightly user upkeep using startup switches in the POA startup file. By default, nightly user upkeep is enabled. Use the --nuuoffset and --rdaboffset switches to specify the start times.

POA Console: You can view the current user upkeep schedule on the Scheduled Events page.

16 Managing the POA

Configuring the POA Console

The web-based POA console is set up automatically when you create a new post office. You can optionally protect the POA console with a user name and password, or use an SSL connection between your web browser and the POA.

1 In the GroupWise Admin console, browse to and click the POA.

2 Click the **Agent Settings** tab, then scroll down to the **HTTP** section.

3 (Conditional) If you want to use an SSL connection for the POA console, which provides optimum security, select **Enabled** or **Required** in the **HTTP SSL** drop-down list.

- **Enabled:** If the POA is configured with a valid SSL certificate, the POA console uses SSL. If a valid SSL certificate is not available, the POA still provides the POA console, but without a secure SSL connection.
- **Required:** The POA does not support the POA console unless a valid SSL certificate has been provided.

For additional instructions about using SSL connections, see "Server Certificates and SSL Encryption" on page 695.

4 If you want to limit access to the POA console, fill in the **HTTP User Name** and **HTTP Password** fields.

Unless you are using SSL, do not use a user name that is synchronized from an LDAP directory (such as NetIQ eDirectory or Microsoft Active Directory). This is because the information passes over the non-secure connection between your web browser and the agent. If you are using SSL, the user name is encrypted and therefore secure.

5 Click **Save**, then click **Close** to return to the main Admin console window.

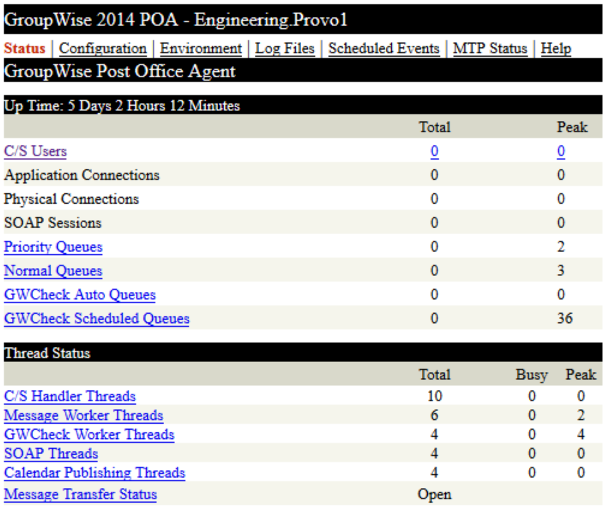
6 Continue with Accessing the POA Console.

Corresponding Startup Switches: You can also use the --httpport, --httpuser, --httppassword, and --httpssl startup switches in the POA startup file to enable and secure the POA console. In addition, you can use the --httprefresh switch to control how often the POA refreshes the information provided to your web browser.

Accessing the POA Console

1 In the GroupWise Admin console, browse to and click the POA.

2 On the **General** tab, click **Launch POA Console**.



GroupWise 2014 POA - Engineering.Provo1

Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help

GroupWise Post Office Agent

Up Time: 5 Days 2 Hours 12 Minutes

	Total	Peak
C/S Users	0	0
Application Connections	0	0
Physical Connections	0	0
SOAP Sessions	0	0
Priority Queues	0	2
Normal Queues	0	3
GWCheck Auto Queues	0	0
GWCheck Scheduled Queues	0	36

Thread Status

	Total	Busy	Peak
C/S Handler Threads	10	0	0
Message Worker Threads	6	0	2
GWCheck Worker Threads	4	0	4
SOAP Threads	4	0	0
Calendar Publishing Threads	4	0	0
Message Transfer Status	Open		

3 In the POA console, you can change some POA configuration settings for the current POA session. You can also stop and start some specific POA threads.

TIP: To access the POA console directly from your web browser, provide the URL where the POA is located by supplying the network address and port number. For example:

```
http://poa_server_address:1677
http://poa_server_address:7181
```

When viewing the POA console, you can specify either the client/server port or the HTTP port.

IMPORTANT: In order to control the POA from the POA console, you must set up authentication for the POA console. For more information, see "Configuring the POA Console" on page 159.

Changing POA Configuration Settings

On the POA console menu, click **Configuration**. Online help on the Configuration page helps you interpret the configuration information being displayed.

If the POA console is password protected as described in "Configuring the POA Console" on page 159, you can click hyperlinked configuration items to change settings for the current agent session.

Controlling the POA MTP Threads

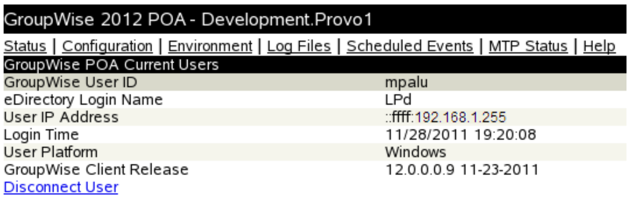
On the Configuration page, click **Message Transfer Protocol.**

On this page, you can restart MTA processing between the POA and the MTA. On the MTP status page, you can restart the send and receive threads separately.

Disconnecting a User Session from the POA

In Online mode, the GroupWise client establishes an active session with the POA. If you disable a user while the user is logged in, it does not terminate the user’s live session with the POA. For more information, see “Disabling and Enabling GroupWise Accounts” on page 473.

After disabling the user in the GroupWise Admin console, you can disconnect the user in the POA console. On the Status page in the POA console, click **C/S Users**, then click **Disconnect User** for the user that you have already disabled in the GroupWise Admin console.



IMPORTANT: When you disable the user in the GroupWise Admin console, the POA must receive the disable event and process it before the user can be disconnected in the POA console. You can see the disable event occur in the POA log file. When you click **Disconnect User** successfully, the user is no longer listed in the POA console. If the user does not disappear from the list after you click **Disconnect User**, wait for the POA to process the disable event, then click **Disconnect User** again. A disconnected user receives an error message stating that GroupWise will exit.

---

17 Monitoring the POA

By monitoring the POA, you can determine whether or not its current configuration is meeting the needs of the post office it services. You have a variety of tools to help you monitor the operation of the POA:

Using the POA Console

The web-based POA console enables you to monitor and control the POA from any location where you have access to a web browser and the Internet. The POA console provides several pages of information to help you monitor the performance of the POA.

Monitoring POA Status

When you first access the POA console, the Status page is displayed. Online help on the Status page helps you interpret the status information being displayed.

Click any hyperlinked status items for additional details. Click **Help** for more information about any field.

Monitoring POA Threads

The POA Status page provides links to detailed POA thread status for the following types of threads:

- C/S handler threads
- Message worker threads
- GWCheck worker threads
- SOAP threads
- Calendar Publishing threads

The **Thread ID** column provides the information you need in order to track a specific thread through one or more POA log files. For more information, see "Viewing and Searching POA Log Files" on page 167.

Tracking Peak Values for Connections, Queue Contents, and Thread Usage

On the **Status** tab in the POA console, the statistics for client/server connections, message queues, and various types of POA threads include peak values. Peak values help you assess whether the current totals represent peaks.

To display the time of day for the peak values, click the number in the **Peak** column on the **C/S User** line.

You can set the peak value refresh interval to Daily, Weekly, Monthly, or Never.

Corresponding Startup Switches: You can also use the --peakrefreshinterval switch in the POA startup file to configure to configure the peak refresh interval.

Listing POA Scheduled Events

On the POA console menu, click **Scheduled Events** to view currently scheduled events and their status information.

QuickFinder indexing and remote downloadable Address Book generation can be controlled using links from the Configuration page, if the POA console is password protected. For more information, see "Configuring the POA Console" on page 159.

The Configuration page also displays information about disk check events and database maintenance events. However, scheduled events must be created and modified using the GroupWise Admin console.

Checking Link Status to the MTA

On the POA console menu, click **MTP Status** to view status information about the link between the POA for the post office and MTA for the domain.

If the POA console is password protected, the **Outbound TCP/IP** link displays the MTA console where you can get status information about the MTA. For more information, see "Configuring the POA Console" on page 159,

The **Hold** link displays the contents of the MTA input queue, so you can find out if messages are waiting for processing by the MTA.

Taking Performance Snapshots

To help you assess the efficiency of the POA, you can configure the POA to gather statistics about CPU utilization, disk reads and writes, thread usage, message processing, and so on.

1. Ensure that the POA console is password protected.

   For instructions, see "Configuring the POA Console" on page 159.
2. In the POA console, on the Configuration page, click **Performance Snapshots** under the **Performance Settings** heading.
3. Select **Start**, then click **Submit**.

   The POA takes a snapshot every 60 seconds.
4. Refresh your browser window to display data as it is collected.
5. Specify the interval at which you want to write data to a file on disk for permanent storage.

   Performance data is saved to the `*mmdd*snap.*nnn*` file, where *mmdd* represents the current month and date and *nnn* starts with 001 and increments each time you enable performance snapshots to start gathering data. The performance data file is stored in the `*post_office*\oftemp` folder in comma-separated value (CSV) format, so that you can bring the data into a spreadsheet program for analysis.
6. (Optional) Specify options to send the performance data to another user via email.

   You can specify to send the performance data **Now**, **At the end of the day**, or **After running for *x* hours**. You must specify the email addresses of the users to whom you want to send the performance data.
7. When you have gathered sufficient performance data, select **Stop**, then click **Submit**.

Because gathering performance data uses POA resources, you should turn the feature off when you have gathered sufficient data. It is turned off automatically when you restart the POA.

8 When you are finished using performance data files, delete them to conserve disk space.

The POA does not automatically clean up old performance data files.

Monitoring SOAP Events

To help you work with third-party listener applications such as the GroupWise Mobility Service, the POA console lists SOAP notifications and SOAP events so that you can monitor the SOAP event traffic through the POA. These options are available if the POA console is password protected, as described in "Configuring the POA Console" on page 159.

- "Listing SOAP Notifications" on page 165
- "Listing SOAP Event Configurations" on page 165

Listing SOAP Notifications

The SOAP Notification List page shows the third-party listener applications that are notified by the POA when SOAP events occur.

1 In the POA console, on the Configuration page, click **SOAP Notification List**.

The columns provide the following information:

UserID: Displays the name of the GroupWise user that is performing the event.

Key: Displays the ID of the event configuration created by the third-party application. The event configuration describes the events that are being tracked for the user, such as creation, deletion, or modification of records.

IP Address: Displays the IP address of the POA where the event took place.

Port: Displays the port number used for communication between the POA and the listener application.

Date/Time: Displays the date and time when the event took place. An asterisk (*) after the date and time indicates that the user has pending notifications. After the notifications have been sent, the asterisk is removed.

Listing SOAP Event Configurations

The Event Configuration List page displays the event configurations that are registered to receive GroupWise events from the POA. An event configuration is listed when an external application such as the GroupWise Mobility Service communicates with the POA and provides information about a specific type of event that it wants to receive.

For example, the GroupWise Mobility Service synchronizes GroupWise data to mobile devices. Whenever a user connects a mobile device to GroupWise through the GroupWise Mobility Service, an event configuration is created for that user and his or her mobile device. If the user has multiple mobile devices, there is an event configuration for each of the user's mobile devices.

1 In the POA console, on the Configuration page, click **Event Configuration List**.

The columns provide the following information:

UserID: Displays the name of the GroupWise user associated with the event configuration.

Key: Displays the ID of the event configuration created by the external application. For example, the GroupWise Connector uses a GroupWise trusted application key.

IP Address: Displays the IP address of the external application that the POA notifies when events take place.

Port: Displays the port number used for communication between the POA and the external application.

Events: Displays the number of events that have transferred from the POA to the external application.

2. To manage the event configuration for a specific user, click the user name.

   The Event Configuration page helps you manage an event configuration and the associated events that are stored in a user's database for an external application such as the GroupWise Mobility Service.

3. Select **Add to Notification List**, then click **Submit** to cause the POA to notify the external application whenever a new GroupWise event needs to be picked up.

4. Select **Show Events**, then click **Submit** to display the currently stored events for the event configuration.

   If the list is long, the external application might not be running.

5. Select **Delete Events**, then click **Submit** to delete any stored events for the event configuration.

   Use this option only when a backlog of events needs to be cleared, such as when a problem occurred with the external application.

6. Click **Delete Event Configuration**, then click **Submit** to delete the displayed event configuration.

   Use this option when the POA no longer needs to send events for the user associated with the event configuration. For example, if there was a problem removing a user from the GroupWise Connector, use this option to remove any residual events associated with the user.

Using POA Log Files

Error messages and other information about POA functioning are written to log files and can be displayed in the POA console. Log files can provide a wealth of information for resolving problems with POA functioning or message flow. This section covers the following subjects to help you get the most from POA log files:

Locating POA Log Files

The default location of the POA log files varies by platform:

Linux:	`/var/log/novell/groupwise/`*`post_office_name`*`.poa`
Windows:	*`post_office`*`\wpcsout\ofs`

You can change the location where the POA creates its log files, as described in Configuring POA Log Settings and Switches.

Configuring POA Log Settings and Switches

When installing or troubleshooting the POA, a logging level of Verbose can be useful. However, when the POA is running smoothly, you can set the logging level down to Normal to conserve disk space occupied by log files.

1 In the GroupWise Admin console, browse to and click the POA.

2 Click the **Log Settings** tab.

3 Set the desired settings for logging.

Log File Path: Browse to and select the folder where you want this POA to store its log files.

Logging Level: Select the amount of data displayed on the POA console and written to the POA log file.

- **Off:** Turns off disk logging and sets the logging level for the POA to its default. Logging information is still displayed in the POA console.
- **Normal:** Displays only the essential information suitable for a smoothly running POA.
- **Verbose:** Displays the essential information, plus additional information that can be helpful for troubleshooting.
- **Diagnostic:** Turns on **Extensive Logging Options** and **SOAP Logging Options** on the POA console Log Settings page.

Maximum Log File Age: Specifies how many days to keep POA log files on disk. The default is 30 days.

Maximum Log Disk Space: Sets the maximum amount of disk space for all POA log files. When the specified disk space is consumed, the POA deletes existing log files, starting with the oldest. The default is 100 MB. The maximum allowable setting is 1000 MB (1 GB).

Corresponding Startup Switches: You can also use the --log, --loglevel, --logdays, --logmax, and --logdiskoff switches in the POA startup file to configure logging.

Viewing and Searching POA Log Files

You can view the contents of the POA log file in the POA console.

1 In the POA console, click **Log Files**.

2 To view a log file, select the log file, then click **View Events**.

3 To search for a specific string, select the log files to search, specify the string in the **Events Containing** field, then click **View Events**.

TIP: To search all log files, select **Select All**.

---

4 To create a new log file, click **Cycle Log**.

On Linux, you can use the `tail` command to monitor a file named *poa*`.currentlog`, where *poa* is the name of the POA eDirectory object. This file is a symbolic link to the current POA log file, so that you do not need to keep track of the exact POA log file name, which includes the log file creation date and an incrementing extension for multiple log files created on the same date.

Interpreting POA Log File Information

On startup, the POA records the POA settings currently in effect. Thereafter, it logs events that take place, including errors.

Because the POA consists of multiple threads, you might find it useful to retrieve the log file into an editor and sort it on the thread ID that follows the date and time information. Sorting groups all messages together for the same POA thread.

Using GroupWise Monitor

GroupWise Monitor is a monitoring and management tool that allows you to monitor GroupWise agents from any location where you are connected to the Internet and have access to a web browser. In addition, GroupWise Monitor can notify you when agent problems arise.

For installation and setup instructions, see "Setting Up GroupWise Monitor" in the *GroupWise 18 Installation Guide*. For usage instructions, see Part XVII, "Monitor," on page 637.

Using Micro Focus Remote Manager

When GroupWise agents are running on Micro Focus Open Enterprise Server (OES), you can use Micro Focus Remote Manager to monitor them. For more information, see the *Micro Focus Remote Manager Administration Guide*.

Using an SNMP Management Console

You can monitor the GroupWise agents from SNMP management and monitoring programs. When properly configured, the GroupWise agents send SNMP traps to network management consoles for display along with other SNMP monitored programs.

Although the GroupWise agents are SNMP-enabled by default, the server where the GroupWise agents are installed must be properly configured to support SNMP, and the agents must also be properly configured. To set up SNMP services, complete the following tasks:

Setting Up SNMP Services for the POA

Select the instructions for the platform where the POA runs:

- "Linux: Setting Up SNMP Services for the POA" on page 168
- "Windows: Setting Up SNMP Services for the POA" on page 169

Linux: Setting Up SNMP Services for the POA

The Linux GroupWise agents are compatible with NET-SNMP. An older version of SNMP called UCD-SNMP cannot be used with the Linux GroupWise agents. NET-SNMP comes with OES, but it does not come with SLES. If you are using SLES, you must update to NET-SNMP in order to use SNMP to monitor the Linux GroupWise agents.

1. Ensure you are logged in as root.
2. If NET-SNMP is not already set up on your Linux server, use the following command to configure SNMP:

```
snmpconf -g basic_setup
```

The `snmpconf` command creates the `snmpd.conf` file in one of the following folders, depending on your version of Linux:

```
/usr/share/snmp
/usr/local/share/snmp
~/.snmp
```

3 Locate the `snmpd.conf` file on your Linux server.
4 In a text editor, open the `snmpd.conf` file and add or uncomment the following lines:

```
dlmod Gwsnmp /opt/novell/groupwise/agents/lib/libgwsnmp.so

export LD_LIBRARY_PATH=/opt/novell/groupwise/agents/lib

export MIBDIRS=/usr/share/snmp/mibs:/opt/novell/groupwise/agents/mibs

export MIBS=ALL
```

5 Save the `snmpd.conf` file and exit the text editor.
6 Restart the SNMP daemon (snmpd) to put the changes into effect.

IMPORTANT: Ensure that the SNMP daemon always starts before the POA starts.

Skip to "Copying and Compiling the POA MIB File" on page 169.

Windows: Setting Up SNMP Services for the POA

SNMP support is automatically installed along with the GroupWise agents. SNMP support is provided for up to instances of each GroupWise agent on the same Windows server. Upon startup, each instance of a GroupWise agent is dynamically assigned a row in its SNMP table. View the contents of the agent MIB for a description of the SNMP variables in the table.

On some versions of Windows Server, the SNMP Service is not included during the initial operating system installation. The SNMP Service can be added either before or after the GroupWise agents are installed on the Windows server.

Continue with Copying and Compiling the POA MIB File.

Copying and Compiling the POA MIB File

An SNMP-enabled GroupWise agent returns information contained in a Management Information Base (MIB). The MIB is an ASCII data structure that defines the information gathered. It also defines the properties that can be monitored and managed on the SNMP-enabled GroupWise agent.

Before you can monitor an SNMP-enabled GroupWise agent, you must compile the agent MIB file using your SNMP management program. GroupWise agent MIB files are located in the `/agents/mibs` folder in your GroupWise software installation.

The MIB file contains all the Trap, Set, and Get variables used for communication between the GroupWise agent and the SNMP management console. The Trap variables provide warnings that point to current and potential problems. The Set variables allow you to configure portions of the application while it is still running. The Get variables display the current status of different processes of the application.

1 Copy the agent MIB file to the location required by your SNMP management program.
2 Compile or import the agent MIB file as required by your SNMP management program.

Continue with Configuring the POA for SNMP Monitoring.

Configuring the POA for SNMP Monitoring

In order for SNMP monitoring programs to monitor the a GroupWise agent, the GroupWise agent must be configured with an SNMP community string.

1. In the GroupWise Admin console, browse to and click the GroupWise agent object.
2. Click the **Agent Settings** tab, then locate the **SNMP Community "Get" String** field.
3. Provide your system SNMP community "Get" string, then click **OK**.
4. Configure the SNMP Service with the same community "Get" string.
5. Restart the GroupWise agent.

   The GroupWise agent should now be visible to your SNMP monitoring program.

18 Optimizing the POA

You can adjust how the POA functions to optimize its performance. Before attempting optimization, you should run the POA long enough to observe its efficiency and its impact on other network applications running on the same server. See Chapter 17, “Monitoring the POA,” on page 163.

Also, remember that optimizing your network hardware and operating system can make a difference in POA performance.

The following topics help you optimize the POA:

Optimizing Client/Server Processing

Adjusting the Number of Client/Server Threads

When the POA is configured with client/server processing enabled, it starts client/server handler threads to respond to current client/server requests, up to the number of threads specified by the **Client/Server Handler Threads** option. To respond to occasional heavy loads, the POA can increase the number of client/server handler threads above the specified amount if CPU utilization is below the threshold established by the **CPU Utilization** setting. When the POA rereads its configuration information, the number of client/server handler threads drops back within the configured limit. You can determine how often this happens by checking the Client/Server Pending Requests History page in the POA console.

If the POA is frequently not keeping up with the client/server requests from GroupWise client users, you can increase the maximum number of client/server handler threads so the POA can create additional threads as needed. The default is 10 client/server handler threads; valid values range from 1 to 99.

If GroupWise client users cannot connect to the POA immediately or if response is sluggish, you can increase the number of threads.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Agent Settings** tab, and locate the **Client/Server** section.
3. Increase the number in the **Client/Server Handler Threads** field to increase the maximum number of threads the POA can create for client/server processing.

   The optimum number of threads for a POA is affected by many factors, including available system resources, number of users in Caching mode, number of users priming Caching mailboxes, and so on.

   Plan on at least one client/server handler thread per 20-30 client/server users. Or, you can increase the number of client/server handler threads in increments of three to five threads until acceptable throughput is reached. Another approach is to set the value high initially and then monitor thread usage with the **C/S Handler Threads** link on the Status page of the POA console. If some of the threads always have a count of 0 (zero), meaning they are never used, you can decrease the number of client/server handler threads accordingly.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --tcpthreads switch in the POA startup file to adjust the number of POA client/server handler threads.

POA Console: The Status page helps you assess whether the POA is currently meeting the client/server needs of the post office. Under the **Thread Status** heading, click **C/S Handler Threads** to display the workload and status of the client/server handler threads.

If the POA console is password protected as described in "Configuring the POA Console" on page 159, you can change the number of client/server handler threads on the Configuration page. Under **Performance Settings**, click **C/S Handler Threads**.

Adjusting the Number of Client/Server Connections

Connections are the number of "sockets" through which client/server requests are communicated from the GroupWise client to the POA.

- **Application connections:** Each GroupWise user uses one application connection when he or she starts GroupWise. Depending on what activities the user is doing in the GroupWise client, additional application connections are used. For example, the GroupWise Address Book and GroupWise Notify use individual application connections. The default maximum number of application connections is 2048. You should plan about 3 to 4 application connections per user, so the default is appropriate for a post office of about 500 users.
- **Physical connections:** Each GroupWise user could have zero or multiple active physical connections. One physical connection can accommodate multiple application connections. Inactive physical connections periodically time out and are then closed by the clients and the POA. The default maximum number of physical connections is 2048. You should plan about 1 to 2 physical connections per user, so the default is appropriate for a post office of about 500 users.

If the POA is configured with too few connections to accommodate the number of users in the post office, the POA can encounter an error condition such as "GWPOA: Application connection table full".

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Agent Settings** tab, and locate the **Client/Server** section.
3. Increase the number in the **Max Physical Connections** field to increase the amount of TCP/IP traffic the POA can accommodate.
4. Increase the number in the **Max App Connections** field to increase the number of activities the attached users can perform concurrently.
5. Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --maxappconns and --maxphysconns switches in the POA startup file to adjust the POA client/server processing.

POA Console: The Status page helps you assess whether the POA is currently meeting the client/server needs of the post office. Under the **Statistics** heading, click **C/S Requests Pending**. You can also manually select multiple log files to search in order to display a history of times during the last 24 hours when the POA was unable to respond immediately to client/server requests.

Optimizing Thread Management

The availability of client/server threads affects a GroupWise user's experience in the GroupWise client. When the POA is working under a heavy load, users can experience degraded performance when sufficient client/server threads are not available. To maintain the best possible performance for GroupWise users, the POA automatically favors client/server processing over message handling. By default, under a heavy load, the POA automatically decreases the number of message handler

threads and increases the number of client/server threads to favor client connections while keeping the total number of threads constant. This behavior benefits users because they are more aware of client performance than they are of messages that they have not yet received.

However, one result of this default behavior is that the message queues can back up during times of heavy client activity. If necessary, you can manually adjust the POA's ratio of client/server threads and message handler threads to help the POA clear out its message queues.

1 Ensure that the POA console is password protected.

   For instructions, see "Configuring the POA Console" on page 159.

2 In the POA console, click **Configuration > Message Worker Threads**.

3 Increase the number in the **Worker Yields to C/S Level** field to increase the amount of time that the POA waits before reallocating message worker threads as client/server threads.

   Increasing this setting configures the POA to continue processing message queues rather than focusing on client/server processing. Valid values range from 0 (zero) to five. Select 0 to turn off the automatic thread adjustments. The settings of 1 through 5 represent increasing amounts of time, but not a specific number of seconds or minutes.

4 Click **Submit** after changing the setting.

   The POA automatically restarts to put the new setting into effect.

5 Experiment with the setting until you achieve a proper balance between client/server processing and message processing.

Optimizing Message File Processing

If the POA is configured for message file processing, it starts the number of threads specified by the **Message Handler Threads** option. Message handler threads deliver messages to users mailboxes. The default number of message handler threads is 6; valid values range from 1 to 20. The default value of 6 is appropriate for a multipurpose POA. The maximum value of 20 is appropriate for a POA that has been customized to process only message files.

The more message threads the POA uses, the faster it can process messages. However, the more threads the POA uses, the fewer resources are available to other processes running on the server.

To adjust the number of POA message handler threads:

1 In the GroupWise Admin console, browse to and click the POA.

2 Click the **Agent Settings** tab and locate the **Message Processing** section.

3 Increase the number in the **Message Handler Threads** field.

   For example, you could increase the number of threads in increments of three to five threads until acceptable throughput is reached. The optimum number of threads for a POA is affected by many factors, including available system resources. The more message handler threads the POA uses, the more incoming messages it can process simultaneously. However, the more threads the POA uses, the fewer threads are available to other processes running on the same server.

4 Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --threads switch in the POA startup file to adjust the number of message handler threads.

POA Console: The Status page helps you assess whether the POA is currently meeting the message file processing needs of the post office. Under the **Thread Status** heading, click **Message Worker Threads** to display the workload and status of the message handler threads.

If the POA console is password protected as described in "Configuring the POA Console" on page 159, you can change the number of message handler threads on the Configuration page. Under **Performance Settings**, click **Message Worker Threads**.

Optimizing Database Maintenance

The POA by default performs a certain amount of database maintenance. In addition, you can create your own customized maintenance events as described in "Scheduling Database Maintenance" on page 154 and "Scheduling Disk Space Management" on page 156.

By default, the POA starts one thread to handle all POA scheduled events and also all usage of the Mailbox/Library Maintenance tool in the GroupWise Admin console.

To adjust the number of POA database maintenance handler threads:

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Maintenance** tab.
3. Increase the number in the **Maintenance Handler Threads** field.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --gwchkthreads switch in the POA startup file to increase the number of POA threads started for database maintenance activities.

POA Console: The Status page helps you assess whether the POA is currently meeting the database maintenance needs of the post office. Under the **Thread Status** heading, click **GWCheck Worker Threads** to display the workload and status of the database maintenance handler threads.

If the POA console is password protected as described in "Configuring the POA Console" on page 159, you can change the number of database maintenance handler threads on the Configuration page. Under **Performance Settings**, click **Maximum GWCheck Worker Threads**.

Optimizing Client Purge Operations

If enough users empty a very large number of items from their mailboxes all at once, the POA can become very busy purging the items, rather than responding to other user requests in a timely manner. Similarly, when many users log in to GroupWise at about the same time (for example, first thing in the morning), many clients might need to start an Auto-Archive task (which includes purge operations as part of the archive task), and this can also make the POA very busy until the purge operations are completed.

By default, the POA is configured to efficiently handle a typical amount of purging. However, if the default configuration is unacceptably slow during periods of heavy purging, you can prevent users' client response time from degrading. You can configure the POA to restrict the amount of purging that can take place concurrently.

1. Ensure that the POA console is password protected.

   For instructions, see "Configuring the POA Console" on page 159.
2. In the POA console, click **Configuration > Mass Purge Items Threshold**.

   The default settings are typically appropriate.
3. (Conditional) If users are experiencing sluggish response time at the beginning of the day, increase the settings until satisfactory response time is achieved.

Purge Items Threshold: Select the maximum number of items that the POA immediately purges from a mailbox. The default number of items to purge immediately is less than 10. Valid values range from 5 to 50.

Max Concurrent Threads Limit: Select the maximum number of concurrent threads that the POA can start for purging batches of items that exceed the Mass Purge Items Threshold setting. The default number of concurrent threads for purging items is 3. Valid values range from 1 to 8.

4 Click **Submit** after changing the setting.

The POA automatically restarts to put the new setting into effect.

Optimizing Calendar Publishing

See “Configuring a POA for Calendar Publishing” in the *GroupWise 18 Installation Guide*.

19 Managing Indexing of Attachment Content

There are several things that you can do to customize how the POA handling indexing of messages and attached documents.

NOTE: To facilitate the Find feature in the GroupWise client, the POA searches unindexed messages as well as those that have already been indexed, so that all messages are immediately available to users whenever they perform a search. The POA does not search unindexed documents, so documents cannot be located using the client Find feature until after indexing has been performed.

For a list of the file types that the POA can index, see *Oracle Outside In Technology Supported Formats* (http://www.oracle.com/technetwork/middleware/content-management/ds-oitfiles-133032.pdf).

Configuring Indexing

By default, the POA indexes messages and documents in the post office every 24 hours at 8:00 p.m. You can modify this interval if users need messages and documents indexed more quickly. To start indexing immediately, see "Controlling Indexing" on page 178.

To adjust the interval at which indexing occurs:

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **QuickFinder** tab.
3. Ensure **Enable QuickFinder Indexing** is selected.
4. In the **Start QuickFinder Indexing** field, specify the number of hours and minutes after midnight you want the POA to start its indexing cycle.

   For example, if you set **QuickFinder Interval** to 6 and **Start QuickFinder Indexing** to 1 hour, indexing cycles occurs at 1:00 a.m., 7:00 a.m., 1:00 p.m., and 7:00 p.m.
5. Decrease the number of hours and minutes in the **QuickFinder Interval** field so indexing occurs more frequently.

   The interval is measured from the start of one indexing cycle to the next, so that indexing starts at regular intervals, no matter how long each indexing session takes. By default, the start point of the cycle is 8:00 p.m.

   To avoid overloading the POA with indexing processing, a maximum of 500 items are indexed per database for each indexing cycle. If a very large number of messages are received regularly, you should configure the POA with frequent indexing cycles in order to get all messages indexed in a timely manner.

   To handle occasional heavy indexing requirements, you can start indexing manually. See "Controlling Indexing" on page 178.
6. Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --qfinterval, --qfintervalinminute, --qfbaseoffset, and --qfbaseoffsetinminute switches in the POA startup file to regulate indexing.

POA Console: If the POA console is password protected as described in “Configuring the POA Console” on page 159, you can control indexing for the current POA session on the Configuration page. Under the **General Settings** heading, click **QuickFinder Indexing**. If indexing is currently in progress, you can check the status of the indexing process on the Scheduled Events page.

Controlling Indexing

GroupWise uses QuickFinder technology to index messages and documents stored in post offices. You can control indexing in the POA console. For example, if you just imported a large number of documents, you could start indexing immediately, rather than waiting for the next scheduled indexing cycle.

1 In the POA console, click **Configuration > QuickFinder Indexing**.

2 Select **Update Indexes Only**, then click **Submit**.

   To avoid overloading the POA with indexing processing, a maximum of 500 items are indexed per database. If a very large number of messages are received regularly, or if a user with a very large mailbox is moved to a different post office (requiring the user’s messages to be added into the new post office indexes), you might need to repeat this action multiple times in order to get all messages indexed.

   QuickFinder indexes are automatically compressed at midnight each night to conserve disk space. You can start compression at any other time from the POA server console. For example, if you just imported and indexed a large number of documents and are running low on disk space, you could compress the indexes immediately, rather than waiting for it to happen at midnight.

3 Select **Compress Indexes Only**, then click **Submit**.

   A variety of other indexing tasks can be done in the POA console. Click **Help** for details.

Configuring the POA with Multiple DVAs for Indexing

The Document Viewer Agent (DVA) converts attached document files from a wide variety of formats into HTML format for indexing by the POA and for viewing in GroupWise WebAccess. You can run up to three DVAs to service conversion requests for a single instance of the POA. Each DVA must be installed on a different server.

1 Set up multiple DVAs in your GroupWise system.

   For instructions, see Chapter 36, “Scaling Your DVA Installation,” on page 363.

2 In the GroupWise Admin console, browse to and click the POA

3 Click the **Document Viewer Agent** tab.

4 Click Add Document Viewer Agent, then select a DVA from the drop-down list.

5 (Optional) Repeat Step 4 to add a third DVA.

6 Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --dva*n*ipaddr, --dva*n*port, and --dva*n*ssl switches in the POA startup file to configure multiple DVAs.

Controlling Maximum Document Conversion Size and Time

By default, the POA sends all attached documents for HTML conversion for indexing, regardless of the size of the document, and by default, the POA waits as long as 10 minutes to receive the HTML version.

You control the maximum document conversion size and time using startup switches in the POA startup file. After you edit the POA startup file, you must restart the POA in order to put the changes into effect.

Use the --dvamaxsize switch to restrict the size of documents that it sends for conversion. Set the --dvamaxsize switch to the maximum document size in kilobytes. For example, you would use 20480 for 20 MB.

Use the --dvamaxtime switch to change the amount of time the POA waits for the HTML version. Set the --dvamaxtime switch to the number of seconds that you want the POA wait. The default is 600 seconds.

Customizing Indexing

By default, the POA indexes 500 items in a user or library database, then moves on to the next database during each QuickFinder indexing cycle. The indexing cycle is established on the **QuickFinder** tab of the POA object. By default, QuickFinder indexing is performed once a day at 8:00 p.m. If a database has more than 500 items that need to be indexed, items beyond 500 wait for the next indexing cycle.

Occasionally, circumstances arise where indexing needs are especially heavy for a short period of time. This can occur when you move users to a different post office or if the QuickFinder indexes for a post office become damaged. Startup switches are available for temporary use in the POA startup file to customize the way the POA handles indexing. In general, they are not intended for long-term use. You might want to set up a separate POA just to handle the temporary indexing needs, and use these switches only with the dedicated indexing POA.

Because the switches are placed in the POA startup file, you must stop and then start the POA to put the settings into effect.

Determining What to Index

You can configure the POA to index just user mailbox contents or just library contents. Use the --qfnousers switch to focus on indexing library contents. Use the --qfnolibs switch to focus on indexing user mailbox contents. Use the --qfnopreproc switch to suppress even the generation of document word lists that are normally written to user databases that reference documents.

When you have a large number of user databases that need to be indexed, you can configure the POA to index a specific range of databases based on user FIDs. For a task of this magnitude, you should run multiple dedicated indexing POAs with each POA configured to process a specific range of databases. Use the --qfuserfidbeg and --qfuserfidend switches to define the range for each POA. You can determine the FID numbers of the databases by listing the user databases (`user`*xxx*`.db`) in the `ofuser` folder. The *xxx* part of the user database name is the FID.

You could also use these switches to single out a specific user database for indexing. Specify the same FID for both switches. To determine a user's FID in the GroupWise client, click **Help > About GroupWise**. In Online mode, the FID is displayed after the user name. In Caching or Remote mode, the FID is the last three characters of the Caching or Remote folder name (for example, `gwstr7bh`). In the GroupWise Admin console, users' FIDs can be displayed in a column on the Users page.

Determining Indexing Priority

The POA carries on many processes at once. You can configure the POA to make indexing a higher or lower priority task than responding to users' activities in their mailboxes. You can also control how many items the POA indexes in each database that it processes. Use the --qflevel switch to control indexing priority.

The table below explains the priority levels:

Priority Level	Description
0	Index a maximum of 1000 items at a time, rather than the default of 500.
1	Index a maximum of 500 items at time, using a low-priority thread. This keeps frequent daytime indexing cycles from interfering with users' activities in their mailboxes.
2	Index a maximum of 1000 items at a time, using a medium-priority thread. This allows additional items in each database to be processed in each indexing cycle. Using a medium-priority thread makes indexing more important than some user activities in mailboxes. Users might notice some slowness in response from the GroupWise client. This is the default setting for the --qflevel switch.
3	Index a maximum of 2000 items at a time, using a high-priority thread. Using a high- priority thread makes indexing more important than many user activities in mailboxes. Users will notice some slowness in response from the GroupWise client. This is warranted only when the immediate completion of indexing is extremely important.
999	Index constantly until all databases have been indexed, then wait until the next indexing cycle set on the **QuickFinder** tab of the POA object before starting to index again.

If you have users who consistently receive more items than are processed during your current daily indexing cycle, you could implement an appropriate --qflevel setting for permanent use.

Reclaiming Disk Space

The POA uses `.idx` files to store compressed indexes. It uses `.inc` files to store incremental indexes that have not yet been compressed. At regular intervals, the POA compresses the contents of the `.inc` files and adds the data to the `.idx` files. Afterwards, it retains the previous `.idx` and `.inc` files for a period of time. Use the --qfdeleteold switch to delete the previous versions of the `.idx` and `.inc` files to conserve disk space during periods of heavy indexing. It is primarily applicable when using --qflevel=1 where indexing is a lower priority task. For --qflevel=2 and --qflevel=3, indexing itself is a higher priority than compression and deletion cleanup tasks.

Preventing Indexing of Specific Document Types

If the Oracle Outside In Technology (http://www.oracle.com/technetwork/middleware/content-management/ds-oitfiles-133032.pdf) used by the POA encounters problems indexing types of files that you receive regularly, you can configure the POA to not pass those files to the DVA for indexing. For example, if you regularly receive coredump files with a `.img` extension and do not want the POA to index them, you can configure the POA to filter them out of the indexing process.

Use the --dvafilter switch in the POA startup file to specify the file extensions that you do not want the POA to index. After you edit the POA startup file, you must restart the POA to put the change into effect.

20 Using POA Startup Switches

You can override settings provided in the GroupWise Admin console by using startup switches in the POA startup file. The default location for the POA startup file is in the post office folder.

When you create a post office and install the POA, an initial POA startup file is created. It is named using the first 8 characters of the post office name with a `.poa` extension. This initial startup file includes the --home startup switch set to the location of the post office folder.

Startup switches specified on the command line override those in the startup file. Startup switches in the startup file override corresponding settings in the GroupWise Admin console. You can view the POA startup file from the Configuration page in the POA console.

The table below summarizes POA startup switches for all platforms and how they correspond to configuration settings in the GroupWise Admin console.

Switch starts with: a b c d e f g h i j k l m n o p q r s t u v w x y z

Linux POA	Windows POA	GroupWise Admin Console Settings
@file_name	*@file_name*	N/A
--adminport	/adminport	N/A
--attemptsresetinterval	/attemptsresetinterval	**Incorrect Login Reset Time**
--certfile	/certfile	**Certificate File**
--cluster	/cluster	N/A
--dhparm	/dhparm	N/A
--dvafilter	/dvafilter	N/A
--dva*n*ipaddr	--dva*n*ipaddr	N/A
--dva*n*port	--dva*n*port	N/A
--dva*n*ssl	--dva*n*ssl	N/A
--dvamaxsize	/dvamaxsize	N/A
--dvamaxtime	/dvamaxtime	N/A
--dvaquarantine	/dvaquarantine	N/A
--enforceclientversion	/enforceclientversion	**Lock Out Older GroupWise Clients**
--evocontrol	/evocontrol	N/A
--externalclientssl	/externalclientssl	**Internet Client/Server SSL**
--gwchkthreads	/gwchkthreads	**Maintenance Handler Threads**
--gwclientreleasedate	/gwclientreleasedate	**Minimum Client Release Date**
--gwclientreleaseversion	/gwclientreleaseversion	**Minimum Client Release Version**
--help	/help	N/A

Linux POA	Windows POA	GroupWise Admin Console Settings
--home	/home	N/A
--httppassword	/httppassword	HTTP Password
--httpport	/httpport	HTTP Port
--httprefresh	/httprefresh	N/A
--httpssl	/httpssl	HTTP SSL
--httpuser	/httpuser	HTTP User Name
--imap	/imap	IMAP
--imapmaxthreads	/imapmaxthreads	Max IMAP Threads
--imapport	/imapport	IMAP Port
--imapreadlimit	/imapreadlimit	N/A
--imapreadnew	/imapreadnew	N/A
--imapssl	/imapssl	IMAP SSL
--imapsslport	/imapsslport	IMAP SSL Port
--incorrectloginattempts	/incorrectloginattempts	Incorrect Logins Allowed
--internalclientssl	/internalclientssl	Local Intranet Client SSL
--intruderlockout	/intruderlockout	Enable Intruder Detection
--ip	/ip	N/A
--keyfile	/keyfile	SSL Key File
--keypassword	/keypassword	SSL Key File Password
--language	/language	N/A
--ldapdisablepwdchg	/ldapdisablepwdchg	Disable LDAP Password Changing
--ldapipaddr	/ldapipaddr	LDAP Server Address
--ldappoolresettime	/ldappoolresettime	LDAP Pool Server Reset Timeout
--ldapport	/ldapport	LDAP Server Address
--ldappwd	/ldappwd	LDAP Password
--ldapssl	/ldapssl	Use SSL
--ldapsslkey	/ldapsslkey	SSL Key File
--ldaptimeout	/ldaptimeout	Inactive Connection Timeout
--ldapuser	/ldapuser	LDAP User Name
--ldapuserauthmethod	/ldapuserauthmethod	User Authentication Method
--lockoutresetinterval	/lockoutresetinterval	Lockout Reset Time
--log	/log	Log File Path
--logdays	/logdays	Max Log File Age

Linux POA	Windows POA	GroupWise Admin Console Settings
--logdiskoff	/logdiskoff	Logging Level
--loglevel	/loglevel	Logging Level
--logmax	/logmax	Max Log Disk Space
--maxappconns	/maxappconns	Max Application Connections
--maxphysconns	/maxphysconns	Max Physical Connections
--mtpinipaddr	/mtpinipaddr	IP Address (POA)
--mtpinport	/mtpinport	Message Transfer Port (POA)
--mtpoutipaddr	/mtpoutipaddr	IP Address (MTA)
--mtpoutport	/mtpoutport	Message Transfer Port (MTA)
--mtpsendmax	/mtpsendmax	Maximum Send Message Size
--mtpssl	/mtpssl	Message Transfer SSL
--name	/name	N/A
--noada	/noada	N/A
--nocache	/nocache	Enable Caching
--noconfig	/noconfig	N/A
--noerrormail	/noerrormail	N/A
--nogwchk	/nogwchk	N/A
--nomf	/nomf	Message File Processing
--nomfhigh	/nomfhigh	Message File Processing
--nomflow	/nomflow	Message File Processing
--nomtp	/nomtp	N/A
--nonuu	/nonuu	Perform User Upkeep
--noqf	/noqf	Enable QuickFinder Indexing
--nordab	/nordab	Generate Address Books for Remote
--norecover	/norecover	Enable Auto DB Recovery
--nosnmp	/nosnmp	Enable SNMP
--notcpip	/notcpip	Enable Client/Server
--nuuoffset	/nuuoffset	Start User Upkeep
--password	/password	Remote Password
--peakrefreshinterval	/peakrefreshinterval	N/A
--port	/port	Client/Server Port
--primingmax	/primingmax	Max Thread Usage for Priming and Moves
--qfbaseoffset	/qfbaseoffset	Start QuickFinder Indexing

Linux POA	Windows POA	GroupWise Admin Console Settings
--qfbaseoffsetinminute	/qfbaseoffsetinminute	**Start QuickFinder Indexing**
--qfdeleteold	/qfdeleteold	N/A
--qfinterval	/qfinterval	**QuickFinder Interval**
--qfintervalinminute	/qfintervalinminute	**QuickFinder Interval**
--qflevel	/qflevel	N/A
--qfnolibs	/qfnolibs	N/A
--qfnopreproc	/qfnopreproc	N/A
--qfnousers	/qfnousers	N/A
--qfuserfidbeg	/qfuserfidbeg	N/A
--qfuserfidend	/qfuserfidend	N/A
--rdaboffset	/rdaboffset	**Start Address Book Generation**
--rights	/rights	N/A
--show	N/A	N/A
--soap	/soap	**Enable SOAP**
--soapmaxthreads	/soapmaxthreads	**Max SOAP Threads**
--soapport	/soapport	**SOAP Port**
--soapsizelimit	/soapsizelimit	N/A
--soapssl	/soapssl	**SOAP SSL**
--soapthreads	/soapthreads	N/A
--sslciphersuite	/sslciphersuite	N/A
--ssloption	/ssloption	N/A
--tcpthreads	/tcpthreads	**Client/Server Handler Threads**
--threads	/threads	**Message Handler Threads**
--user	/user	N/A

@startup_file_name

Specifies the location of the POA startup file. The POA startup file is created in the post office folder and is named after the post office, with a `.poa` extension. The POA startup file includes the --home switch.

	Linux POA	Windows POA
Syntax:	@[/*dir*/]*file*	@[*drive*:][*dir*\\]*file*
Example:	./gwpoa @../share/lnxpost.poa	gwpoa.exe @sales.poa gwpoa.exe @d:\agt\sales.poa

--adminport

Specifies the port number used for the POA to communicate with the GroupWise Admin Service. The default port number is 9711.

	Linux POA	Windows POA
Syntax:	--adminport *port_number*	/adminport-*port_number*
Example:	--adminport 9721	/adminport-9721

--attemptsresetinterval

Specifies the length of time during which unsuccessful login attempts are counted, leading to lockout. The default is 30 minutes; valid values range from 15 to 60. See "Configuring Intruder Detection" on page 153.

	Linux POA	Windows POA
Syntax:	--attemptsresetinterval *minutes*	/attemptsresetinterval-*minutes*
Example:	--attemptsresetinterval 45	/attemptsresetinterval-60

See also --intruderlockout, --incorrectloginattempts, and --lockoutresetinterval.

--certfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the POA and other programs. See "Securing the Post Office with SSL Connections to the POA" on page 152.

	Linux POA	Windows POA
Syntax:	--certfile /*dir*/*file*	/certfile-[*drive*:]*dir**file* /certfile-*svr**sharename**dir**file*
Example:	--certfile /certs/gw.crt	/certfile-\ssl\gw.crt /certfile-m:\ssl\gw.crt certfile-\\\\server2\c\ssl\gw.crt

See also --keyfile and --keypassword.

--cluster

Informs the POA that it is running in a cluster. When communicating with a clustered POA, the GroupWise client extends the retry period for reconnection. A clustered POA automatically binds to the IP address configured for the POA object even if the **Bind Exclusively to TCP/IP Address** option is not selected on the POA Agent Settings tab in the GroupWise Admin console. This prevents

unintended connections to other IP addresses, such as the loopback address or the node's physical IP address. For information about clustering the POA, see "Clustering" in the *GroupWise 18 Interoperability Guide*.

	Linux POA	Windows POA
Syntax:	--cluster	/cluster

See also --ip.

--dhparm

Specifies a Diffie-Hellman cipher parameters file used for SSL/TLS to replace the default parameters set by GroupWise. GroupWise uses default Diffie-Hellman parameters of 2048 bits to generate the DH key. A valid DH parameter is in PEM format.

	Linux POA	Windows POA
Syntax:	--dhparm *directory*/*pemfile*	/dhparm *directory*/*pemfile*
Example:	--dhparm /var/tmp/dh.pem	/dhparm C:\temp\dh.pem

--dvafilter

Sets the file name extensions for attached documents that you do not want the POA to hand off to the DVA for conversion into HTML format. See "Preventing Indexing of Specific Document Types" on page 181.

To specify multiple file name extensions, specify a comma-delimited list, surrounded by quotation marks (").

	Linux POA	Windows POA
Syntax:	--dvafilter *file_extension*	/dvafilter-*file_extension*
	--dvafilter "*file_extension*,*file_extension*"	/dvafilter-"*file_extension*,*file_extension*"
Example:	--dvafilter img	/dvafilter-"img,arc"

--dva*n*ipaddr

Specifies the IP address of a DVA that the POA can use to convert documents into HTML format for indexing. You can configure the POA to communicate with up to three DVAs. In the switch, replace *n* with 1, 2, or 3 to identify multiple DVAs. See "Configuring the POA with Multiple DVAs for Indexing" on page 178.

	Linux POA	Windows POA
Syntax:	--dva*n*ipaddr *ip_address*	/dva*n*ipaddr-*ip_address*
Example:	--dva1ipaddr 172.17.5.18	/dva2ipaddr-172.17.5.19

See also --dva*n*port and --dva*n*ssl.

--dva*n*port

Specifies the port number used for the POA to communicate with the corresponding DVA. The default port number is 8301. In the switch, replace *n* with 1, 2, or 3 to identify multiple DVAs. See "Configuring the POA with Multiple DVAs for Indexing" on page 178.

	Linux POA	Windows POA
Syntax:	--dva*n*port *port_number*	/dva*n*port-*port_number*
Example:	--dva2port 8302	/dva3port-8303

See also --dva*n*ipaddr and --dva*n*ssl.

--dva*n*ssl

Sets the availability of SSL communication between the POA and the corresponding DVA. Valid values are `enable` and `disable`. SSL is disabled by default. In the switch, replace *n* with 1, 2, or 3 to identify multiple DVAs. See "Configuring the POA with Multiple DVAs for Indexing" on page 178.

	Linux POA	Windows POA
Syntax:	--dva*n*ssl *setting*	/dva*n*ssl-*setting*
Example:	--dva2ssl enable	/dva3ssl-enable

See also --dva*n*ipaddr and --dva*n*port.

--dvamaxsize

Sets the maximum size for attached documents that the POA hands off to the DVA for conversion into HTML format so that the documents can be indexed. By default, there is no maximum size limit. See "Controlling Maximum Document Conversion Size and Time" on page 179.

	Linux POA	Windows POA
Syntax:	--dvamaxsize *kilobytes*	/dvamaxsize-*kilobytes*
Example:	--dvamaxsize 20480	/dvamaxsize-40960

See also --dvamaxtime.

--dvamaxtime

Sets the maximum time that the POA waits to receive documents converted into HTML by the DVA. The default is 600 seconds (10 minutes). See "Controlling Maximum Document Conversion Size and Time" on page 179.

	Linux POA	Windows POA
Syntax:	--dvamaxtime *seconds*	/dvamaxtime-*seconds*
Example:	--dvamaxtime 20480	/dvamaxtime-40960

See also --dvamaxsize.

--dvaquarantine

Enables the document quarantine where the POA places documents that the DVA fails to convert into HTML for indexing.

	Linux POA	Windows POA
Syntax:	--dvaquarantine	/dvaquarantine

--enforceclientversion

Enforces the minimum client release version and/or date so that users of older clients are forced to update in order to access their GroupWise mailboxes. Valid settings are version, date, both, and disabled. See "Checking What GroupWise Clients Are in Use" on page 148.

	Linux POA	Windows POA
Syntax:	--enforceclientversion *setting*	/enforceclientversion-*setting*
Example:	--enforceclientversion date	/enforceclientversion-both

See also --gwclientreleasedate, and --gwclientreleaseversion.

--evocontrol

Determines which versions of Evolution are allowed to access the post office. Users might experience problems using Evolution to connect to their GroupWise mailboxes if they are using Evolution 2.6.0 or earlier. In addition, earlier versions of Evolution can cause high utilization on GroupWise servers.

To encourage users to update to the latest version of Evolution, you can use the --evocontrol switch to configure the POA to allow only specified versions of Evolution. For information about configuring a post office to support Evolution, see "Supporting SOAP Clients" on page 148.

	Linux POA	Windows POA
Syntax:	--evocontrol-Evolution-*version.date* --evocontrol-Evolution-Data-Server-*version-date*	/evocontrol-Evolution-*version.date* /evocontrol-Evolution-Data-Server-*version-date*
Example:	--evocontrol Evolution-1.10-2006-12-04 --evocontrol Evolution-Data-Server-1.10-2006-12-04	/evocontrol-Evolution-1.10-2006-12-04 /evocontrol-Evolution-Data-Server-1.10-2006-12-04

You can put as many as 10 entries in the startup file, so that you can list as many as 10 versions of Evolution. Entries beyond 10 are ignored. You can view the current entries at the POA console with the other SOAP settings. The POA log file lists the settings in the Soap Session section.

--externalclientssl

Sets the availability of SSL communication between the POA and GroupWise clients that are running outside your firewall. Valid values are enabled, required, and disabled. See "Securing the Post Office with SSL Connections to the POA" on page 152.

	Linux POA	Windows POA
Syntax:	--externalclientssl *setting*	/externalclientssl-*setting*
Example:	--externalclientssl disabled	/externalclientssl-required

See also --certfile, --keyfile, --keypassword, and --port.

--gwchkthreads

Specifies the number of threads the POA starts for Mailbox/Library Maintenance activities. The default is 4; valid values range from 1 to 8. See "Optimizing Database Maintenance" on page 174.

	Linux POA	Windows POA
Syntax:	--gwchkthreads *number*	/gwchkthreads-*number*
Example:	--gwchkthreads 6	/gwchkthreads-8

See also --nogwchk.

--gwclientreleasedate

Specifies the date of the approved GroupWise client software for your system. See "Checking What GroupWise Clients Are in Use" on page 148.

	Linux POA	Windows POA
Syntax:	--gwclientreleasedate *mm-dd-yyyy*	/gwclientreleasedate-*mm-dd-yyyy*
Example:	--gwclientreleasedate 10-24-2008	/gwclientreleasedate-10-24-2008

See also --gwclientreleaseversion and --enforceclientversion.

--gwclientreleaseversion

Specifies the version of the approved GroupWise client software for your system. See "Checking What GroupWise Clients Are in Use" on page 148.

	Linux POA	Windows POA
Syntax:	--gwclientreleaseversion *n.n.n*	/gwclientreleaseversion-*n.n.n*
Example:	--gwclientreleaseversion 6.5.6	/gwclientreleaseversion-7.0.0

See also --gwclientreleasedate and --enforceclientversion.

--help

Displays the POA startup switch Help information. When this switch is used, the POA does not start.

	Linux POA	Windows POA
Syntax:	--help	/help or /?
Example:	./gwpoa --help	gwpoa.exe /help

--home

Specifies the post office folder, where the POA can access message and user databases. There is no default location. You must use this switch in order to start the POA.

	Linux POA	Windows POA
Syntax:	--home /*dir*	/home-[*drive*:]*dir* /home-*svr**sharename**dir*
Example:	--home /gwsystem/sales	/home-\sales /home-m:\sales /home-\\\\server2\c\sales

If you specify a UNC path with the --home switch when you run the POA as a Windows service, you must configure the POA service to run under a specific Windows user account. If you specify a local folder or a mapped drive, you can configure the POA service to run under the local system account. However, running as the Administrator account is highly recommended.

--httppassword

Specifies the password for the POA to prompt for before allowing POA status information to be displayed in your web browser. Do not use an existing eDirectory password because the information passes over the non-secure connection between your web browser and the POA. See "Using the POA Console" on page 163.

	Linux POA	Windows POA
Syntax:	--httppassword *unique_password*	/httppassword-*unique_password*
Example:	--httppassword AgentWatch	/httppassword-AgentWatch

See also --httpuser, --httpport, --httprefresh, and --httpssl.

--httpport

Sets the HTTP port number used for the POA to communicate with your web browser. The default is 7181; the setting must be unique. See "Using the POA Console" on page 163.

	Linux POA	Windows POA
Syntax:	--httpport *port_number*	/httpport-*port_number*
Example:	--httpport 7183	/httpport-7184

See also --httpuser, --httppassword, --httprefresh, and --httpssl.

--httprefresh

Specifies the rate at which the POA refreshes the status information in your web browser. The default is 60 seconds. See "Using the POA Console" on page 163.

	Linux POA	Windows POA
Syntax:	--httprefresh *seconds*	/httprefresh-*seconds*
Example:	--httprefresh 90	/httprefresh-120

See also --httpuser, --httppassword, --httpport, and --httpssl.

--httpssl

Sets the availability of secure SSL communication between the POA and the POA console displayed in your web browser. Valid values are enabled and disabled. See “Securing the Post Office with SSL Connections to the POA” on page 152.

	Linux POA	Windows POA
Syntax:	--httpssl *setting*	/httpssl-*setting*
Example:	--httpssl enabled	/httpssl-enabled

See also --certfile, --keyfile, and --keypassword.

--httpuser

Specifies the user name for the POA to prompt for before allowing POA status information to be displayed in a web browser. Providing a user name is optional. Do not use an existing eDirectory user name because the information passes over the non-secure connection between your web browser and the POA. See “Using the POA Console” on page 163.

	Linux POA	Windows POA
Syntax:	--httprefresh *unique_name*	/httprefresh-*unique_name*
Example:	--httpuser GWWebCon	/httpuser-GWWebCon

See also --httppassword, --httpport, --httprefresh, and --httpssl.

--imap

Enables IMAP so that the POA can communicate with IMAP clients. Valid settings are enabled and disabled. See “Supporting IMAP Clients” on page 147.

	Linux POA	Windows POA
Syntax:	--imap enabled or disabled	/imap-enabled or disabled
Example:	--imap disabled	/imap-enabled

See also --imapmaxthreads, --imapport, --imapreadlimit, --imapreadnew, --imapssl, and --imapsslport.

--imapmaxthreads

Specifies the maximum number of IMAP threads the POA can create to service IMAP clients. The default is 40. This setting is appropriate for most systems. See "Supporting IMAP Clients" on page 147.

	Linux POA	Windows POA
Syntax:	--imapmaxthreads *number*	/imapmaxthreads-*number*
Example:	--imapmaxthreads 30	/imapmaxthreads-35

See also --imap, --imapport, --imapreadlimit, --imapreadnew, --imapssl, and --imapsslport.

--imapreadlimit

Specifies in thousands the maximum number of messages that can be downloaded by an IMAP client. For example, specifying 10 represents 10,000. The default is 20,000. The maximum allowed limit is 65. The server caches all downloaded items, so setting a high limit could consume more server resources than you would prefer the POA to use.

	Linux POA	Windows POA
Syntax:	--imapreadlimit *number*	/imapreadlimit-*number*
Example:	--imapreadlimit 20	/imapreadlimit-50

See also --imap, --imapmaxthreads, --imapport, --imapreadnew, --imapssl, and --imapsslport.

--imapreadnew

By default, the IMAP agent reads items in a folder from the oldest to the newest. As a result, if a folder contains more items than are allowed by the --imapreadlimit setting, users receive the older items but not the newer items. Enable this switch so that the POA reads items from the newest to the oldest. This ensures that users receive all their new items in a timely manner.

	Linux POA	Windows POA
Syntax:	--imapreadnew	/imapreadnew

See also --imap, --imapmaxthreads, --imapreadlimit, --imapport, --imapssl, and --imapsslport.

--imapport

Sets the TCP port number used for the POA to communicate with IMAP clients when using a non-SSL connection. The default is 143. See "Supporting IMAP Clients" on page 147.

	Linux POA	Windows POA
Syntax:	--imapport *port_number*	/imapport-*port_number*

	Linux POA	Windows POA
Example:	--imapport 146	/imapport-147

See also --imap, --imapmaxthreads, --imapreadlimit, --imapreadnew, --imapssl, and --imapsslport.

--imapssl

Sets the availability of secure SSL communication between the POA and IMAP clients. Valid settings are enable and disable. See "Securing the Post Office with SSL Connections to the POA" on page 152.

	Linux POA	Windows POA
Syntax:	--imapssl *setting*	/imapssl-*setting*
Example:	--imapssl enable	/imapssl-enable

See also --imap, --imapmaxthreads, --imapport, --imapreadlimit, --imapreadnew, and --imapsslport.

--imapsslport

Sets the TCP port number used for the POA to communicate with IMAP clients when using an SSL connection. The default is 993. See "Supporting IMAP Clients" on page 147.

	Linux POA	Windows POA
Syntax:	--imapsslport *port_number*	/imapsslport-*port_number*
Example:	--imapsslport 995	/imapsslport-996

See also --imap, --imapmaxthreads, --imapport, --imapreadlimit, --imapreadnew, and --imapssl.

--incorrectloginattempts

Specifies the number of unsuccessful login attempts after which lockout occurs. The default is 5 attempts; valid values range from 3 to 10. See "Configuring Intruder Detection" on page 153.

	Linux POA	Windows POA
Syntax:	--incorrectloginattempts *number*	/incorrectloginattempts-*number*
Example:	--incorrectloginattempts 10	/incorrectloginattempts-10

See also --intruderlockout, --attemptsresetinterval, and --lockoutresetinterval.

--internalclientssl

Sets the availability of secure SSL communication between the POA and GroupWise clients that are running inside your firewall. Valid values are enabled, required, and disabled. See "Securing the Post Office with SSL Connections to the POA" on page 152.

	Linux POA	Windows POA
Syntax:	--internalclientssl *setting*	/internalclientssl-*setting*
Example:	--internalclientssl required	/internalclientssl-required

See also --certfile, --keyfile, --keypassword, and --port.

--intruderlockout

Turns on intruder lockout processing, using defaults that can be overridden by the --incorrectloginattempts, --attemptsresetinterval, and --lockoutresetinterval switches. See "Configuring Intruder Detection" on page 153.

	Linux POA	Windows POA
Syntax:	--intruderlockout	/intruderlockout

--ip

Binds the POA to a specific IP address when the server where it runs uses multiple IP addresses, such as in a clustering environment. The specified IP address is associated with all ports used by the POA (HTTP, IMAP, LDAP, and so on.) Without the --ip switch, the POA binds to all available IP addresses and users can access the post office through all available IP addresses. See "Binding the POA to a Specific IP Address" on page 144.

	Linux POA	Windows POA
Syntax:	--ip *IP_address* --ip "*full_DNS_name*"	/ip-*IP_address* /ip-"*full_DNS_name*"
Example:	--ip 172.16.5.18 --ip "poasvr.provo.novell.com"	/ip-172.16.5.18 /ip-"poasvr.provo.novell.com"

See also --cluster.

--keyfile

Specifies the full path to the private file used to provide secure SSL communication between the POA and other programs. See “Securing the Post Office with SSL Connections to the POA” on page 152.

	Linux POA	Windows POA
Syntax:	--keyfile /*dir*/*file*	/keyfile-[*drive*:]*dir**file* /keyfile-*svr**sharename**dir**file*
Example:	--keyfile /certs/gw.key	/keyfile-\ssl\gw.key /keyfile-m:\ssl\gw.key /keyfile-\\\\server2\c\ssl\gw.key

See also --certfile and --keypassword.

--keypassword

Specifies the password used to encrypt the private SSL key file when it was created. See “Securing the Post Office with SSL Connections to the POA” on page 152.

	Linux POA	Windows POA
Syntax:	--keypassword *password*	/keypassword-*password*
Example:	--keypassword gwssl	/keypassword-gwssl

See also --certfile and --keyfile.

--language

Specifies the language to run the POA in, using a two-letter language code. You must install the POA in the selected language in order for the POA to display in the selected language.

The initial default is the language used in the post office. If that language has not been installed, the second default is the language used by the operating system. If that language has not been installed, the third default is English. You only need to use this switch if you need to override these defaults.

	Linux POA	Windows POA
Syntax:	--language *code*	/language-*code*
Example:	--language de	/language-fr

Contact your local Micro Focus sales office for information about language availability. See Chapter 7, “Multilingual GroupWise Systems,” on page 85 for a list of language codes.

--ldapdisablepwdchg

Prevents GroupWise users from changing their LDAP passwords by using the Password dialog box in the GroupWise client. See "Providing LDAP Authentication for GroupWise Users" on page 153.

	Linux POA	Windows POA
Syntax:	--ldapdisablepwdchg	/ldapdisablepwdchg

See also --ldapipaddr, --ldapport, --ldapuser, --ldappwd, --ldapuserauthmethod, --ldapssl, --ldapsslkey, and --ldaptimeout.

--ldapipaddr

Specifies the LDAP server's network address as either an IP address or a DNS hostname. You can specify multiple network addresses to provide failover capabilities for your LDAP servers. See "Specifying Failover LDAP Servers (Non-SSL Only)" on page 83.

	Linux POA	Windows POA
Syntax:	--ldapipaddr *network_address*	/ldapipaddr-*network_address*
Example:	--ldapipaddr 172.16.5.19 --ldapipaddr server1 server2	/ldapipaddr-172.16.5.20 /ldapipaddr-server1 server2

If you specify multiple LDAP servers, use a space between each address. When so configured, the POA tries to contact the first LDAP server in order to authenticate a user to GroupWise. If that LDAP server is down, the POA tries the next LDAP server in the list, and so on until it is able to authenticate.

See also --ldapport, --ldapuser, --ldappwd, --ldapuserauthmethod, --ldapdisablepwdchg, --ldapssl, --ldapsslkey, and --ldaptimeout.

--ldappoolresettime

Specifies the number of minutes between the time when the POA receives an error response from a pooled LDAP server and the time when that LDAP server is reinstated into the pool of available LDAP servers. The default is 5 minutes; valid values range from 1 to 30. See "Configuring a Pool of LDAP Servers" on page 83.

	Linux POA	Windows POA
Syntax:	--ldappoolresettime *minutes*	/ldappoolresettime-*minutes*
Example:	--ldappoolresettime 20	/ldappoolresettime-30

--ldapport

Specifies the port number that the LDAP server listens on for authentication. The default is 389. See "Providing LDAP Authentication for GroupWise Users" on page 153.

	Linux POA	Windows POA
Syntax:	--ldapport *port_number*	/ldapport-*port_number*
Example:	--ldapport 391	/ldapport-392

See also --ldapipaddr, --ldapuser, --ldappwd, --ldapuserauthmethod, --ldapdisablepwdchg, --ldapssl, --ldapsslkey, and --ldaptimeout.

--ldappwd

Provides the password for the LDAP user that the POA uses to log in to the LDAP server. See "Providing LDAP Authentication for GroupWise Users" on page 153.

	Linux POA	Windows POA
Syntax:	--ldappwd *LDAP_password*	/ldappwd-*LDAP_password*
Example:	--ldappwd gwldap	/ldappwd-gwldap

See also --ldapipaddr, --ldapport, --ldapuser, --ldapuserauthmethod, --ldapdisablepwdchg, --ldapssl, --ldapsslkey, and --ldaptimeout.

--ldapssl

Indicates to the POA that the LDAP server it is logging in to is using SSL. See "Providing LDAP Authentication for GroupWise Users" on page 153.

	Linux POA	Windows POA
Syntax:	--ldapssl	/ldapssl

See also --ldapipaddr, --ldapport, --ldapuser, --ldappwd, --ldapuserauthmethod, --ldapdisablepwdchg, --ldapsslkey and --ldaptimeout.

--ldapsslkey

Specifies the full path to the SSL key file used with LDAP authentication. See "Providing LDAP Authentication for GroupWise Users" on page 153.

	Linux POA	Windows POA
Syntax:	--ldapsslkey */dir/file*	/ldapsslkey-[*drive*:]*dir**file* /ldapsslkey-*svr**sharename**dir**file*

	Linux POA	Windows POA
Example:	--ldapsslkey /certs/gwkey.der	/ldapsslkey-\ldap\gwkey.der /ldapsslkey-m:\ldap\gwkey.der /ldapsslkey-\\server2\c\ldap\gwkey.der

See also --ldapipaddr, --ldapport, --ldapuser, --ldappwd, --ldapuserauthmethod, --ldapdisablepwdchg, --ldapssl and --ldaptimeout.

--ldaptimeout

Specifies the number of seconds that the POA connection to the LDAP server can be idle before the POA drops the connection. The default is 30 seconds. See "Providing LDAP Authentication for GroupWise Users" on page 153.

	Linux POA	Windows POA
Syntax:	--ldaptimeout *seconds*	/ldaptimeout-*seconds*
Example:	--ldaptimeout 70	/ldaptimeout-80

See also --ldapipaddr, --ldapport, --ldapuser, --ldappwd, --ldapuserauthmethod, --ldapdisablepwdchg, --ldapssl, and --ldapsslkey.

--ldapuser

Specifies the user name that the POA can use to log in to the LDAP server in order to authenticate GroupWise client users. See "Providing LDAP Authentication for GroupWise Users" on page 153.

	Linux POA	Windows POA
Syntax:	--ldapuser *LDAP_user_ID*	/ldapuser-*LDAP_user_ID*
Example:	--ldapuser GWAuth	/ldapuser-GWAuth

See also --ldapipaddr, --ldapport, --ldappwd, --ldapuserauthmethod, --ldapdisablepwdchg, --ldapssl, and --ldapsslkey, and --ldaptimeout.

--ldapuserauthmethod

Specifies the LDAP user authentication method you want the POA to use when accessing an LDAP server. Valid settings are bind and compare. See "Providing LDAP Authentication for GroupWise Users" on page 153.

	Linux POA	Windows POA
Syntax:	--ldapuserauthmethod *method*	/ldapuserauthmethod-*method*
Example:	--ldapuserauthmethod bind	/ldapuserauthmethod-compare

See also --ldapuser, --ldapipaddr, --ldapport, --ldappwd, --ldapdisablepwdchg, --ldapssl, and --ldapsslkey, and --ldaptimeout.

--lockoutresetinterval

Specifies the length of time the user login is disabled after lockout. The default is 30 minutes; the minimum setting is 15; there is no maximum setting. The login can also be manually re-enabled in the GroupWise Admin console on the **Account** tab of the User object. If --lockoutresetinterval is set to 0 (zero), the login must be re-enabled manually in the GroupWise Admin console. See “Configuring Intruder Detection” on page 153.

	Linux POA	Windows POA
Syntax:	--lockoutresetinterval *minutes*	/lockoutresetinterval-*minutes*
Example:	--lockoutresetinterval 60	/lockoutresetinterval-90

See also --intruderlockout, --incorrectloginattempts, and --attemptsresetinterval.

--log

Specifies the folder where the POA stores its log files. The default location varies by platform.

Linux:	`/var/log/novell/groupwise/`*`post_office_name`*`.poa`
Windows:	*`post_office`*`\wpcsout\ofs`

For more information, see “Using POA Log Files” on page 166.

	Linux POA	Windows POA
Syntax:	--log /*dir*	/log-[*drive*:]*dir* /log-*svr**sharename**dir*
Example:	--log /gwsystem/logs	/log-\agt\log /log-m:\agt\log /log-\\\\server2\c\mail\agt\log

You typically find multiple log files in the specified folder. The first four characters represent the date. The next three characters identify the agent. A three-digit extension allows for multiple log files created on the same day. For example, a log file named `0518poa.001` indicates that it is a POA log file, created on May 18. If you restarted the POA on the same day, a new log file is started, named `0518poa.002`.

See also --loglevel, --logdiskoff, --logdays, and --logmax.

--logdays

Specifies how many days to keep POA log files on disk. The default log file age is 30 days. The valid range is from 1 to 350 days. See “Using POA Log Files” on page 166.

	Linux POA	Windows POA
Syntax:	--logdays *days*	/logdays-*days*
Example:	--logdays 45	/logdays-60

See also --log, --loglevel, --logdiskoff, and --logmax.

--logdiskoff

Turns off disk logging for the POA so no information about the functioning of the POA is stored on disk. The default is for logging to be turned on. See “Using POA Log Files” on page 166.

	Linux POA	Windows POA
Syntax:	--logdiskoff	/logdiskoff

See also --loglevel.

--loglevel

Controls the amount of information logged by the POA. Logged information is displayed in the log message box and written to the POA log file during the current agent session.

The default is Normal, which displays only the essential information suitable for a smoothly running POA. Use Verbose to display the essential information, plus additional information helpful for troubleshooting. Verbose logging does not degrade POA performance, but log files saved to disk consume more disk space when verbose logging is in use. Diagnostic logging turns on **Extensive Logging Options** and **SOAP Logging Options** on the POA console Log Settings page. See “Using POA Log Files” on page 166.

	Linux POA	Windows POA
Syntax:	--loglevel *level*	/loglevel-*level*
Example:	--loglevel verbose	/loglevel-diagnostic

See also --log, --logdiskoff, --logdays, and --logmax.

--logmax

Sets the maximum amount of disk space for all POA log files. When the specified disk space is consumed, the POA deletes existing log files, starting with the oldest. The default is 102400 KB (100 MB). The maximum allowable setting is 102400000 (1 GB). Specify 0 (zero) for unlimited disk space. See “Using POA Log Files” on page 166.

	Linux POA	Windows POA
Syntax:	--logmax *kilobytes*	/logmax-*kilobytes*
Example:	--logmax 130000	/logmax-16000

See also --log, --loglevel, --logdiskoff, and --logdays.

--maxappconns

Sets the maximum number of application connections allowed between the POA and the GroupWise clients run by GroupWise users. The default maximum number of application connections is 2048. See “Adjusting the Number of Client/Server Connections” on page 172.

	Linux POA	Windows POA
Syntax:	--maxappconns *number*	/maxappconns-*number*
Example:	--maxappconns 4096	/maxappconns-5120

See also --maxphysconns.

--maxphysconns

Sets the maximum number of physical TCP/IP connections allowed between the POA and the GroupWise clients run by GroupWise users. The default maximum number of physical connections is 2048. See “Adjusting the Number of Client/Server Connections” on page 172.

	Linux POA	Windows POA
Syntax:	--maxphysconns *number*	/maxphysconns-*number*
Example:	--maxphysconns 4096	/maxphysconns-5120

See also --maxappconns.

--mtpinipaddr

Specifies the network address of the server where the POA runs, as either an IP address or a DNS hostname.

	Linux POA	Windows POA
Syntax:	--mtpinipaddr *network_addr*	/mtpinipaddr-*network_addr*
Example:	--mtpinipaddr 172.16.5.19	/mtpinipaddr-172.16.5.20
	--mtpinipaddr server2	/mtpinipaddr-server3

See also --mtpinport, --mtpoutipaddr, --mtpoutport, --mtpsendmax, and --nomtp.

--mtpinport

Sets the message transfer port number the POA listens on for messages from the MTA. The default is 7101.

	Linux POA	Windows POA
Syntax:	--mtpinport *port_number*	/mtpinport-*port_number*
Example:	--mtpinport 7202	/mtpinport-7203

See also --mtpinipaddr, --mtpoutipaddr, --mtpoutport, --mtpsendmax, and --nomtp.

--mtpoutipaddr

Specifies the network address of the server where the MTA for the domain runs, as either an IP address or a DNS hostname.

	Linux POA	Windows POA
Syntax:	--mtpoutipaddr *network_address*	/mtpoutipaddr-*network_address*
Example:	--mtpoutipaddr 172.16.5.19 --mtpoutipaddr server3	/mtpoutipaddr-172.16.5.19 /mtpoutipaddr-server4

See also --mtpinipaddr, --mtpinport, --mtpoutport, --mtpsendmax, and --nomtp.

--mtpoutport

Specifies the message transfer port number the MTA listens on for messages from the POA. The default is 7100.

	Linux POA	Windows POA
Syntax:	--mtpoutport *port_number*	/mtpoutport-*port_number*

	Linux POA	Windows POA
Example:	--mtpoutport 7300	/mtpoutport-7400

See also --mtpinipaddr, --mtpinport, --mtpoutipaddr, --mtpsendmax, and --nomtp.

--mtpsendmax

Sets the maximum size in megabytes for messages being sent outside the post office. By default, messages of any size can be transferred to the MTA. See "Restricting Message Size between Post Offices" on page 149.

	Linux POA	Windows POA
Syntax:	--mtpsendmax *megabytes*	/mtpsendmax-*megabytes*
Example:	--mtpsendmax 4	/mtpsendmax-6

See also --mtpinipaddr, --mtpinport, --mtpoutipaddr, --mtpoutport, and --nomtp.

--mtpssl

Sets the availability of secure SSL communication between the POA and its MTA. Valid settings are enabled and disabled. See "Securing the Post Office with SSL Connections to the POA" on page 152.

	Linux POA	Windows POA
Syntax:	--mtpssl *setting*	/mtpssl-*setting*
Example:	--mtpssl enabled	/mtpssl-enabled

See also --certfile, --keyfile and --keypassword.

--name

Specifies the object name of the POA object in the post office. If you have multiple POAs configured for the same post office, you must use this switch to specify which POA configuration to use when the POA starts.

	Linux POA	Windows POA
Syntax:	--name *object_name*	/name-*object_name*
Example:	--name POA2	/name-POA2

--noada

Disables the POA admin thread.

The POA admin thread must run for at least one POA for each post office. However, it can be disabled for POAs with specialized functioning where the database update and repair activities of the POA admin thread could interfere with other, more urgent processing.

	Linux POA	Windows POA
Syntax:	--noada	/noada

Historical Note: In GroupWise 5.2 and earlier, a separate agent, the Administration Agent (ADA), handled the functions now consolidated into the POA admin thread. Hence the switch name, --noada.

--nocache

Disables database caching. The default is for caching to be turned on. Use this switch if your backup system cannot back up open files.

	Linux POA	Windows POA
Syntax:	--nocache	/nocache

--noconfig

Ignores any configuration information provided for the POA in the GroupWise Admin console and uses only settings from the POA startup file. The default is for the POA to use the information provided in the GroupWise Admin console, overridden as needed by settings provided in the startup file or on the command line.

	Linux POA	Windows POA
Syntax:	--noconfig	/noconfig

--noerrormail

Prevents problem files from being sent to the GroupWise administrator. The default is for error mail to be sent to the administrator. See "Receiving Notifications of Agent Problems" on page 242.

	Linux POA	Windows POA
Syntax:	--noerrormail	/noerrormail

--nogwchk

Turns off Mailbox/Library Maintenance processing for the POA. The default is for the POA to perform Mailbox/Library Maintenance tasks requested in the GroupWise Admin console and configured as POA scheduled events.

	Linux POA	Windows POA
Syntax:	--nogwchk	/nogwchk

See also --gwchkthreads.

--nomf

Turns off all message file processing for the POA. The default is for the POA to process all message files.

	Linux POA	Windows POA
Syntax:	--nomf	/nomf

See also --nomfhigh and --nomflow.

--nomfhigh

Turns off processing high priority messages files (message queues 0 and 1).

	Linux POA	Windows POA
Syntax:	--nomfhigh	/nomfhigh

See also --nomf and --nomflow.

--nomflow

Turns off processing lower priority messages files (message queues 2 through 7).

	Linux POA	Windows POA
Syntax:	--nomflow	/nomflow

See also --nomf and --nomfhigh.

--nomtp

Disables Message Transfer Protocol, so that a TCP/IP link cannot be used between the POA and the MTA.

	Linux POA	Windows POA
Syntax:	--nomtp	/nomtp

See also --mtpinipaddr, --mtpinport, --mtpoutipaddr, --mtpoutport, and --mtpsendmax.

--nonuu

Disables nightly user upkeep. See “Configuring Nightly User Upkeep” on page 157.

	Linux POA	Windows POA
Syntax:	--nonuu	/nonuu

See also --nuuoffset.

--noqf

Disables the periodic QuickFinder indexing done by the POA. The default is for periodic indexing to be turned on. See “Configuring Indexing” on page 177.

	Linux POA	Windows POA
Syntax:	--noqf	/noqf

See also --qfinterval, --qfintervalinminute, --qfbaseoffset, and --qfbaseoffsetinminute.

--nordab

Disables daily generation of the GroupWise Address Book for Remote users. See “Configuring Nightly User Upkeep” on page 157.

	Linux POA	Windows POA
Syntax:	--nordab	/nordab

See also --rdaboffset.

--norecover

Disables automatic database recovery. The default is for automatic database recovery to be turned on.

If the POA detects a problem with a database when automatic database recovery has been turned off, the POA notifies the administrator, but it does not recover the problem database. The administrator can then recover or rebuild the database as needed. See Chapter 42, “Maintaining Domain and Post Office Databases,” on page 395.

	Linux POA	Windows POA
Syntax:	--norecover	/norecover

--nosnmp

Disables SNMP for the POA. The default is to have SNMP enabled. See “Using an SNMP Management Console” on page 168.

	Linux POA	Windows POA
Syntax:	--nosnmp	/nosnmp

--notcpip

Disables TCP/IP communication for the POA. The default is to have TCP/IP communication enabled. Use this switch if you do not want this POA to communicate with GroupWise clients using TCP/IP.

	Linux POA	Windows POA
Syntax:	--notcpip	/notcpip

--nuuoffset

Specifies the number of hours after midnight for the POA to start performing user upkeep. The default is 1 hour; valid values range from 0 to 23. See “Configuring Nightly User Upkeep” on page 157.

	Linux POA	Windows POA
Syntax:	--nuuoffset *hours*	/nuuoffset-*hours*
Example:	--nuuoffset 3	/nuuoffset-4

See also --nonuu.

--password

Provides the password for the POA to use when accessing post offices or document storage areas on remote servers. You can also provide user and password information on the Post Office **Settings** tab in the GroupWise Admin console.

	Linux POA	Windows POA
Syntax:	--password *network_password*	/password-*network_password*
Example:	--password GWise	/password-GWise

See also --user.

--peakrefreshinterval

Sets the refresh interval for the peak values that are displayed in the POA console. The default is daily. Valid values are daily, weekly, monthly, or never. For more information, see "Tracking Peak Values for Connections, Queue Contents, and Thread Usage" on page 163.

	Linux POA	Windows POA
Syntax:	--peakrefreshinterval daily|weekly|monthly|never	/peakrefreshinterval-daily|weekly|monthly|never
Example:	--peakrefreshinterval weekly	/peakrefreshinterval-never

--port

Sets the TCP port number used for the POA to communicate with GroupWise clients in client/server access mode. The default is 1677.

	Linux POA	Windows POA
Syntax:	--port *port_number*	/port-*port_number*
Example:	--port 1679	/port-1680

See also --ip.

--primingmax

Sets the maximum number of client/server handler threads that POA can use for priming users' Caching mailboxes. The default is 30 per cent. See "Supporting Forced Mailbox Caching" on page 149.

	Linux POA	Windows POA
Syntax:	--primingmax *percentage*	/primingmax-*percentage*
Example:	--primingmax 50	/primingmax-60

See also --tcpthreads.

--qfbaseoffset

Specifies the number of hours after midnight for the POA to start its indexing cycle as specified by the --qfinterval or --qfintervalinminute switch. The default is 20 hours (meaning at 8:00 p.m.); valid values range from 0 to 23. See “Configuring Indexing” on page 177.

	Linux POA	Windows POA
Syntax:	--qfbaseoffset *hours*	/qfbaseoffset-*hours*
Example:	--qfbaseoffset 2	/qfbaseoffset-3

See also --qfbaseoffsetinminute, --qfinterval, --qfintervalinminute, and --noqf.

--qfbaseoffsetinminute

Specifies the number of minutes after midnight for the POA to start its indexing cycle as specified by the --qfinterval or --qfintervalinminute switch. The default is 20 hours (1200 minutes, meaning at 8:00 p.m.). The maximum setting is 1440 (24 hours). See “Configuring Indexing” on page 177.

	Linux POA	Windows POA
Syntax:	--qfbaseoffsetinminute *minutes*	/qfbaseoffsetinminute-*minutes*
Example:	--qfbaseoffset 45	/qfbaseoffset-90

See also --qfbaseoffset, --qfinterval, --qfintervalinminute, and --noqf.

--qfdeleteold

Deletes previous versions of QuickFinder `.idx` and `.inc` files to conserve disk space during periods of heavy indexing. In general, it is applicable for use only with --qflevel=1, where indexing activities are a lower priority task than user activities in their mailboxes. See “Reclaiming Disk Space” on page 180.

	Linux POA	Windows POA
Syntax:	--qfdeleteold	/qfdeleteold

See also --qflevel, --qfnolibs, --qfnopreproc, --qfnousers, --qfusefidbeg, and --qfuserfidend.

--qfinterval

Specifies the interval in hours for the POA to update the QuickFinder indexes in the post office. The default is 24 hours. See "Configuring Indexing" on page 177.

	Linux POA	Windows POA
Syntax:	--qfinterval *hours*	/qfinterval-*hours*
Example:	--qfinterval-6	/qfinterval-2

See also --qfbaseoffset, --qfbaseoffsetinminute, --qfintervalinminute, and --noqf.

--qfintervalinminute

Specifies the interval in minutes for the POA to update the QuickFinder indexes in the post office. The default is 24 hours (1440 minutes). See "Configuring Indexing" on page 177.

	Linux POA	Windows POA
Syntax:	--qfintervalinminute *minutes*	/qfintervalinminute-*minutes*
Example:	--qfintervalinminute 30	/qfintervalinminute-120

See also --qfinterval, --qfbaseoffset, --qfbaseoffsetinminute, and --noqf.

--qflevel

Customizes the way the POA performs indexing. Valid levels are 0 through 3 and 999. The default level is 2 (or 1000 items at a time). See "Determining Indexing Priority" on page 180.

	Linux POA	Windows POA
Syntax:	--qflevel *level*	/qflevel-*level*
Example:	--qflevel 3	/qflevel-999

The table below explains the priority levels:

Priority Level	Description
0	Index a maximum of 1000 items at a time.
1	Index a maximum of 500 items at time, using a low-priority thread. This keeps frequent daytime indexing cycles from interfering with users' activities in their mailboxes.
2	Index a maximum of 1000 items at a time, using a medium-priority thread. This allows additional items in each database to be processed in each indexing cycle. Using a medium-priority thread makes indexing more important than some user activities in mailboxes. Users might notice some slowness in response from the GroupWise client. This is the default setting for the --qflevel switch.

Priority Level	Description
3	Index a maximum of 2000 items at a time, using a high-priority thread. Using a high- priority thread makes indexing more important than many user activities in mailboxes. Users will notice some slowness in response from the GroupWise client. This is warranted only when the immediate completion of indexing is extremely important.
999	Index constantly until all databases have been indexed, then wait until the next indexing cycle set on the **QuickFinder** tab of the POA object before starting to index again.

See also --qfdeleteold, --qfnolibs, --qfnopreproc, --qfnousers, --qfusefidbeg, and --qfuserfidend.

--qfnolibs

Suppresses QuickFinder indexing of documents in libraries in favor of indexing user mailbox contents. For full suppression, use --qfnopreproc as well. See "Determining What to Index" on page 179

	Linux POA	Windows POA
Syntax:	--qfnolibs	/qfnolibs

See also --qfdeleteold, --qflevel, --qfnopreproc, --qfnousers, --qfusefidbeg, and --qfuserfidend.

--qfnopreproc

Suppresses generation of document word lists that are normally written to user databases when libraries are indexed. Use with --qfnolibs. See "Determining What to Index" on page 179.

	Linux POA	Windows POA
Syntax:	--qfnopreproc	/qfnopreproc

See also --qfdeleteold, --qflevel, --qfnolibs, --qfnousers, --qfusefidbeg, and --qfuserfidend.

--qfnousers

Suppresses QuickFinder indexing of user mailbox contents in favor of indexing documents in libraries. See "Determining What to Index" on page 179.

	Linux POA	Windows POA
Syntax:	--qfnousers	/qfnouser

See also --qfdeleteold, --qflevel, --qfnolibs, --qfnopreproc, --qfusefidbeg, and --qfuserfidend.

--qfuserfidbeg

Specifies the beginning of a range of FIDs associated with user databases (`user`*`xxx`*`.db`) that you want to index. The *xxx* in the user database file name is the FID. To determine what FIDs are in use, list the contents of the `ofuser` folder in the post office folder. See "Determining What to Index" on page 179.

	Linux POA	Windows POA
Syntax:	--qfuserfidbeg *fid*	/qfuserfidbeg-*fid*
Example:	--qfuserfidbeg 7ck	/qfuserfidbeg-7j6

See also --qfdeleteold, --qflevel, --qfnolibs, --qfnopreproc, --qfnousers, and --qfuserfidend.

--qfuserfidend

Specifies the end of a range of FIDs associated with user databases (`user`*`xxx`*`.db`) that you want to index. The *xxx* in the user database file name is the FID. To determine what FIDs are in use, list the contents of the `ofuser` folder in the post office folder. See "Determining What to Index" on page 179.

	Linux POA	Windows POA
Syntax:	--qfuserfidend *fid*	/qfuserfidend-*fid*
Example:	--qfuserfidbeg x9c	/qfuserfidbeg-zzf

If you want to index just one user database, use the same FID with the --qfuserfidbeg switch and the --qfuserfidend switch. To determine a user's FID, click **Help > About GroupWise** in the GroupWise client. In Online mode, the FID is displayed after the user name. In Caching or Remote mode, the FID is the last three characters of the Caching or Remote folder name (for example, `gwstr7bh`).

See also --qfdeleteold, --qflevel, --qfnolibs, --qfnopreproc, --qfnousers, and --qfuserfidbeg.

--rdaboffset

Specifies the number of hours after midnight for the POA to generate the daily copy of the GroupWise Address Book for Remote users. The default is 0; valid values range from 0 to 23. See "Configuring Nightly User Upkeep" on page 157.

	Linux POA	Windows POA
Syntax:	--rdaboffset *hours*	/rdaboffset-*hours*
Example:	--rdaboffset 3	/rdaboffset-4

See also --nordab.

--rights

Verifies that the POA has the required network rights or permissions to all folders where it needs access in the post office folder.

When it is started with this switch, the POA lists folders it is checking, which can be a lengthy process. Use this switch on an as needed basis, not in the POA startup file. If the POA encounters inadequate rights or permissions, it indicates the problem and shuts down.

	Linux POA	Windows POA
Syntax:	--rights	/rights

--show

Starts the POA with a server console user interface. The agent user interface requires that the X Window System and Open Motif are running on the Linux server.

By default, no user interface is provided for the agents on Linux. An agent that runs with a user interface cannot be managed in the GroupWise Admin console.

The --show startup switch can be used on the command line or in the `gwha.conf` file used by the GroupWise High Availability Service. It cannot be placed in the agent startup file.

	Linux POA	Windows POA
Syntax:	--show	N/A

--soap

Enables SOAP so that the POA can communicate with SOAP clients. Valid settings are enabled and disabled. See "Supporting SOAP Clients" on page 148.

	Linux POA	Windows POA
Syntax:	--soap enabled or disabled	/soap-enabled or disabled
Example:	--soap enabled	/soap-disabled

See also --soapmaxthreads, --soapport, --soapsizelimit, --soapssl, and --soapthreads.

--soapmaxthreads

Specifies the maximum number of SOAP threads the POA can create to service SOAP clients. The default is 4; the maximum is 40. This setting is appropriate for most systems. See "Supporting SOAP Clients" on page 148.

	Linux POA	Windows POA
Syntax:	--soapmaxthreads *number*	/soapmaxthreads-*number*

	Linux POA	Windows POA
Example:	--soapmaxthreads 20	/soapmaxthreads-30

See also --soap, --soapport, --soapsizelimit, --soapssl, and --soapthreads.

--soapport

Sets the TCP port number used for the POA to communicate with SOAP clients. The default is 7191. See "Supporting SOAP Clients" on page 148.

	Linux POA	Windows POA
Syntax:	--soapport *port_number*	/soapport-*port_number*
Example:	--soapport 146	/soapport-147

See also --soap, --soapmaxthreads, --soapsizelimit, --soapssl, and --soapthreads.

--soapsizelimit

Sets the maximum amount of data that the POA can return in a single request from a SOAP client. The default is 1024 KB (1 MB), which is the recommended setting. The maximum allowed setting is 65534 (64 MB). Specify 0 (zero) if you do not want the POA to check the data size. See "Supporting SOAP Clients" on page 148.

	Linux POA	Windows POA
Syntax:	--soapsizelimit *kilobytes*	/soapsizelimit-*kilobytes*
Example:	--soapsizelimit 2048	/soapsizelimit-2048

See also --soap, --soapmaxthreads, --soapport, --soapssl, and --soapthreads.

--soapssl

Sets the availability of secure SSL communication between the POA and SOAP clients. Valid settings are enable and disable. See "Securing the Post Office with SSL Connections to the POA" on page 152.

	Linux POA	Windows POA
Syntax:	--soapssl *setting*	/soapssl-*setting*
Example:	--soapssl enable	/soapssl-enable

See also --soap, --soapmaxthreads, --soapport, --soapsizelimit, and --soapthreads.

--soapthreads

Sets the initial number of SOAP threads that the POA starts to service SOAP clients. The default is 4. The POA automatically starts additional threads as needed. See "Supporting SOAP Clients" on page 148.

	Linux POA	Windows POA
Syntax:	--soapthreads *number*	/soapthreads-*number*
Example:	--soapthreads 8	/soapthreads-10

See also --soap, --soapmaxthreads, --soapport, --soapsizelimit, and --soapssl.

--sslciphersuite

Sets the SSL cipher suites used by the Archive Agent, the Messaging Agent, and Messenger clients. The cipher list must be in OpenSSL format. For more information on OpenSSL format, see Cipher List Format (https://www.openssl.org/docs/apps/ciphers.html#CIPHER-LIST-FORMAT)

	Linux POA	Windows POA
Syntax:	--sslciphersuite *"setting"*	/sslciphersuite-*"setting*"
Example:	--sslciphersuite "HIGH:!AECDH:!EXP:@STRENGTH"	/sslciphersuite-"HIGH:!AECDH:!EXP:@STRENGTH"

--ssloption

Specify a specific SSL protocol to disable. By specifying SSL_OP_NO_TLSv1, GroupWise will disable TLSv1 support. Specify additional options by adding the SSL key work separated by a comma.

	Linux POA	Windows POA
Syntax:	--ssloption *SSL_protocol*	/ssloption *SSL_protocol*
Example:	--ssloption SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1	/ssloption SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1

--tcpthreads

Specifies the maximum number of client/server handler threads the POA can create to service client/server requests. The default is 10; valid values range from 1 to 99. Plan on about one client/server handler thread per 20-30 client/server users. See "Adjusting the Number of Client/Server Threads" on page 171.

	Linux POA	Windows POA
Syntax:	--tcpthreads *number*	/tcpthreads-*number*

	Linux POA	Windows POA
Example:	--tcpthreads 30	/tcpthreads-50

See also --primingmax.

--threads

Specifies the maximum number of message handler threads the POA can create. The default is 8; valid values range from 1 to 20. See "Optimizing Message File Processing" on page 173.

	Linux POA	Windows POA
Syntax:	--threads *number*	/threads-*number*
Example:	--threads 15	/threads-20

--user

Provides the network user ID for the POA to use when accessing post offices and/or document storage areas on remote servers. You can also provide user and password information on the Post Office Settings tab in the GroupWise Admin console.

	Linux POA	Windows POA
Syntax:	--user *linux_user_ID*	/user-*windows_user_ID*
Example:	--user GWAgents	/user-GWAgents

Linux:	On OES Linux, the *linux_user_ID* is a Linux-enabled user that the POA can use to log in to the remote OES Linux server. On SLES Linux, it is a standard Linux user.
Windows:	The *windows_user_ID* is a user that the POA can use to log in to the remote Windows server.

See also --password.

Windows Note: The Windows POA gains access to the post office folder when it starts. However, a particular user might attempt to access a remote document storage area to which the POA does not yet have a drive mapping available. By default, the POA attempts to map a drive using the same user ID and password it used to access the post office folder. If the user ID and password for the remote storage area are different from the post office, use the --user and --password switches to specify the needed user ID and password. You can also provide user and password information on the Post Office Settings tab in the GroupWise Admin console. However, it is preferable to use the same user ID and password on all servers where the POA needs access.

V Message Transfer Agent

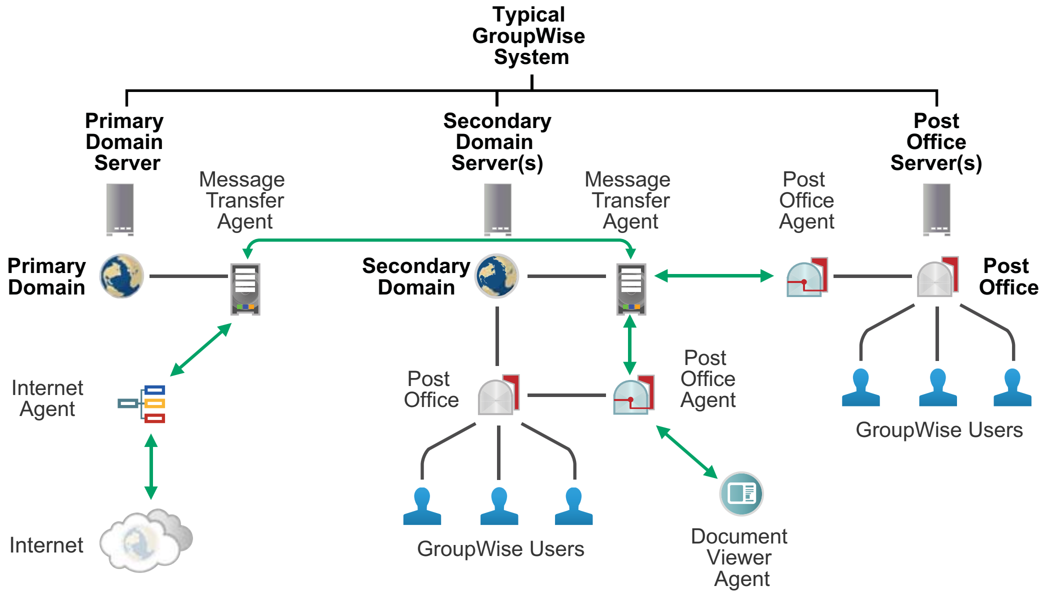
For a complete list of port numbers used by the MTA, see "Message Transfer Agent Port Numbers" on page 728.

For detailed Linux-specific MTA information, see Appendix C, "Linux Basics for GroupWise Administration," on page 735.

21 Understanding Message Transfer between Domains and Post Offices

The Domain and the MTA in Your GroupWise System

A domain organizes post offices into a logical grouping for routing and administration purposes in your GroupWise system. Messages are transferred between post offices and domains by the MTA.



Domain and MTA Representation in the GroupWise Admin Console

In the GroupWise Admin console, domains are listed on the Overview page, along with their agents and post offices.

Information Stored in the Domain

No messages are stored in the domain folder on the server, so GroupWise client users do not need access to the domain folder. The only person who needs file access to the domain folder is the GroupWise administrator.

Domain Database

The domain database (`wpdomain.db`) contains all administrative information for the domain, including:

- Address information about all GroupWise objects (such as users, resources, and post offices in the domain)
- System configuration and linking information for the domain's MTA
- Address and message routing information to other domains

The first domain you create is the primary domain. In the primary domain, the `wpdomain.db` file contains all administrative information for your entire GroupWise system (all its domains, post offices, users, and so on). Because the `wpdomain.db` file in the primary domain is so crucial, you should back it up regularly and keep it secure. See "Backing Up a Domain" on page 421.

You can re-create your entire GroupWise system from the primary domain `wpdomain.db` file; however, if the primary domain `wpdomain.db` file becomes unusable, you can no longer make administrative updates to your GroupWise system.

Secondary domains are automatically synchronized to match the primary domain.

Agent Input/Output Queues in the Domain

Each domain contains agent input/output queues where messages are deposited and picked up for processing by the MTA.

For a mapped or UNC link between domains, the MTA requires read/write access rights to its input/output queues in the other domains. For a TCP/IP link, no access rights are required because messages are communicated by way of TCP/IP.

MTA Input Queue in the Domain

The MTA input queue in the local domain (*domain*`\wpcsin`) is where MTAs for other domains deposit user messages for the local MTA to route to local post offices or to route to other domains. Thus, the MTA input queue in the local domain is the output queue for the MTAs in many other domains.

The MTA does not have an output queue for user messages in the local domain. Because its primary task is routing messages, the local MTA has output queues in all post offices in the domain. See "POA Input Queue in the Post Office" on page 138. The local MTA also has output queues in all domains to which it is directly linked.

MTA Output Queue in the Domain

The MTA output queue in the local domain (*domain*`\wpcsout\ads`) is where the MTA deposits administrative messages from other domains for the MTA admin thread to pick up.

MTA Admin Thread Input Queue in the Domain

The MTA admin thread input queue (*domain*`\wpcsout\ads`) is, of course, the same as the MTA output queue in the local domain. The MTA admin thread picks up administrative messages deposited in the queue by the MTA and updates the domain database.

MTA Admin Thread Output Queue in the Domain

The MTA admin thread output queue (`domain\wpcsin`) is the same as the MTA input queue in the local domain. The MTA admin thread deposits administrative messages in the queue for replication to other domains.

Role of the Message Transfer Agent

You must run an MTA for each domain. The MTA:

- Routes messages between post offices in the local domain.
- Routes messages between domains.
- Routes messages to and from GWIAs that connect your GroupWise system to the Internet.
- Controls the size of messages that can pass across links.

  See "Restricting Message Size between Domains" on page 230.
- Updates the domain database (`wpdomain.db`) whenever GroupWise users, resources, post offices, or other GroupWise objects are added, modified, or deleted.
- Replicates updates to all domains and post offices throughout your GroupWise system. This keeps the Address Book up-to-date for all GroupWise users.
- Synchronizes GroupWise user information with LDAP directory user information.

  See "Configuring User Synchronization for an LDAP Directory" on page 80.
- Synchronizes GroupWise object information throughout your GroupWise system as needed.
- Detects and repairs invalid information in the domain database (`wpdomain.db`).
- Provides logging and statistics about GroupWise message flow.

  See "Enabling MTA Message Logging" on page 228.

Link Configuration between Domains and Post Offices

In GroupWise, a link is defined as the information required to route messages between domains, post offices, and gateways in a GroupWise system. Links are created and configured when new domains, post offices, and gateways are created.

For more specific information about how domains are linked to each other, and about how domains and post offices are linked, see Chapter 10, "Managing the Links between Domains and Post Offices," on page 101.

22 Configuring the MTA

For MTA system requirements, see "Hardware and Operating System Requirements" in the *GroupWise 18 Installation Guide*. For detailed instructions about installing and starting the MTA for the first time, see in the *GroupWise 18 Installation Guide*.

As your GroupWise system grows and evolves, you will probably need to modify MTA configuration to meet changing system needs. The following topics help you configure the MTA:

- Chapter 22, "Configuring the MTA," on page 227
  - Creating an MTA Object in the GroupWise Admin Console
  - Configuring the MTA in the GroupWise Admin Console
  - Binding the MTA to a Specific IP Address
  - Enabling MTA Message Logging
- "Configuring Domain Access" on page 229
  - Securing the Domain with SSL Connections to the MTA
  - Restricting Message Size between Domains
  - Configuring a Routing Domain
- "Configuring User Synchronization" on page 232
  - Configuring LDAP User Synchronization
  - Configuring Exchange Address Book Synchronization
  - Configuring the LDAP Server Capabilities

Performing Basic MTA Configuration

MTA configuration information is stored as properties of its MTA object. The following topics help you modify the MTA object in the GroupWise Admin console and change MTA configuration to meet changing system configurations:

Creating an MTA Object in the GroupWise Admin Console

The initial MTA object is automatically created when you create a new domain. You can have only one MTA for a domain. You cannot create an MTA object in the GroupWise Admin console unless the original MTA object is accidentally deleted.

Configuring the MTA in the GroupWise Admin Console

The advantage to configuring the MTA in the GroupWise Admin console, as opposed to using startup switches in an MTA startup file, is that the settings can be easily edited from any location where the Admin console is available.

1. In the GroupWise Admin console, browse to and click the MTA.
2. For information about each tab and field, click **Help**.

   The context-sensitive help topics link to the related sections of this guide, where you can determine which MTA startup switch corresponds to each MTA setting in the GroupWise Admin console. Some MTA configuration can be done only using a startup file. For more information, see in Chapter 26, "Using MTA Startup Switches," on page 247.

Binding the MTA to a Specific IP Address

If the MTA runs on a server that has multiple IP addresses, you can cause the MTA to bind to a specific IP address. The specified IP address is associated with all ports used by the MTA. Without an exclusive bind, the MTA binds to all IP addresses available on the server.

IMPORTANT: If you bind the MTA (or POA) to a specific IP address, the Admin Service is also bound to that IP address.

---

1 In the GroupWise Admin console, browse to and click the MTA.
2 Click the **Agent Settings** tab, and locate the **Network Address** section.
3 Select **Bind Exclusively to TCP/IP Address**.
4 Click **Save**, then click **Close** to return to the main Admin console window.

TIP: To determine from the command line whether an MTA is bound to a specific IP address, use the following command:

`gwadminutil dbinfo /path_to_domain`

If an IP address is listed, the MTA is bound to that address. If `0.0.0.0` displays, the MTA is not bound to any IP address.

Corresponding Startup Switches: You can also use the --ip switch in the MTA startup file to bind the MTA to a specific IP address.

Enabling MTA Message Logging

Message logging is turned off by default, because it causes the MTA to use additional CPU and disk resources. However, gathering information about message traffic on your GroupWise system lets you perform many valuable tasks, including:

- Tracking messages
- Gathering statistics to help optimize your GroupWise system
- Billing customers for messages delivered
- Tracking messages from the MTA console and from GroupWise Monitor

When you enable MTA message logging, the MTA stores data about GroupWise message traffic as it processes messages. The stored data is then available for use by the MTA console Message Tracking option and by the GroupWise Monitor Message Tracking Report option. In addition, third-party programs can produce customized billing, tracking, and statistical reports based on the information stored in the database.

To enable MTA message logging:

1 In the GroupWise Admin console, browse to and click the MTA.
2 Click the **Log Settings** tab.
3 In the **Message Logging** field, select a logging level to turn message logging on.
4 In the **Message Log Path** field, specify the full path of the file where the MTA will record the logging information.
5 Select the types of information you want to track:

Correlate Delivery Status Reports: Select this option to maintain the relationship between user messages and their corresponding delivery status reports in the logged information.

Collect Delivery Status Reports: Select this option to log delivery status reports as well as user messages.

Collect Other Status Reports: Select this option to log user-requested information about messages sent, such as indicating that messages have been opened or deleted by the recipients.

Track Administrative Messages: Select this option to log administrative messages such as database updates.

6 In the **Delete Reports After** field, specify the number of days to retain reports on disk. Reports are automatically deleted after the specified time has passed.

7 Click **Save**, then click **Close** to return to the main Admin console window.

8 For instructions about using the data that the MTA collects, see "Tracking Messages" on page 238 and "Message Tracking Report" on page 663.

Corresponding Startup Switches: You can also use the --messagelogsettings, --messagelogpath, --messagelogdays, and --messagelogmaxsize switches in the MTA startup file to configure MTA message logging.

Configuring Domain Access

Although users do not access the domain as they use the GroupWise client, their messages often pass through domains while traveling from one post office to another.

Securing the Domain with SSL Connections to the MTA

Secure Sockets Layer (SSL) ensures secure communication between the MTA and other programs by encrypting the complete communication flow between the programs. By default, the MTA is enabled to use SSL connections, but SSL connections are not required.

For background information about SSL and how to set it up on your system, see "Server Certificates and SSL Encryption" on page 695.

To configure the MTA to use SSL:

1 In the GroupWise Admin console, browse to and click the MTA.

2 Click the **SSL Settings** tab.

3 (Conditional) If you need to generate a new self-signed certificate for the MTA:

The GroupWise Admin Service generates a certificate signing request (CSR) and a private key file, and then sends them to the GroupWise certificate authority (CA) on the primary domain. The CA issues the requested certificate, which is then returned to the local server.

3a Click **Generate Certificate**.

3b Specify and confirm the password for the private key file for the new SSL certificate, then click **OK**.

The newly created SSL certificate and private key files display on the **SSL Settings** tab.

3c Click **Save** to save the SSL certificate and key files.

4 (Conditional) If you already have an SSL certificate and key file for the MTA:

4a In the **SSL Certificate File** field, click the **Browse** icon.

4b Click **Upload Local File to Server**, then click **Browse**.

4c Browse to and select the SSL certificate file on your local workstation.

You can use certificate files in the PEM, PFX, CRT, B64, or CER format.

4d Click **Upload** to upload the certificate file into the GroupWise `certificates` folder on the server where the POA is running.

4e Click **OK**.

4f In the **SSL Key File** field, browse to, select, and upload the private key file, then click **OK**.

4g Click **Save** to save the SSL certificate and key files.

5 To enable or require SSL connections with the POA, with other MTAs, and with the MTA console, click the **Agent Settings** tab.

6 To enable or require an SSL connection between the MTA and the POA, and between this MTA and other MTAs, select **Enabled** or **Required** in the **Message Transfer SSL** drop-down list.

The POA must also use SSL for the connection to be secure. See "Securing the Post Office with SSL Connections to the POA" on page 152.

IMPORTANT: To prevent closed links between agents, select **Enabled** when you are initially configuring agents for SSL. Select **Required** for tighter security only after all agents are successfully using SSL.

---

7 To enable SSL between the MTA and the MTA console, select **Enabled** or **Required** in the **HTTP SSL** drop-down list.

8 Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: You can also use the --certfile, --keyfile, --keypassword, --httpssl, and --msgtranssl switches in the MTA startup file to configure the MTA to use SSL.

MTA Console: You can list which connections the MTA is using SSL for from the Links page. Click **View TCP/IP Connections** to display the list if TCP/IP links.

Restricting Message Size between Domains

You can configure the MTA to restrict the size of messages that users are permitted to send outside the domain.

1 In the GroupWise Admin console, click **System > Link Configuration**.

2 In the **Maximum Send Message Size** field, specify in megabytes the size of the largest message you want users to be able to send outside the post office.

IMPORTANT: If you have also set a message size limit for your GWIAs, as described in "Creating a Class of Service" on page 281, ensure that the MTA message size limit is equal to or greater than the GWIA message size limit.

---

3 (Conditional) If you want to delay large messages, specify the size in megabytes for message files the MTA can process immediately in the **Delay Message Size** field.

If a message file exceeds the delay message size, the message file is moved into the low priority (6) message queue, where only one MTA thread is allocated to process very large messages. This arrangement allows typical messages to be processed promptly, while delaying large

messages that exceed the specified size. The result is that large messages do not slow down processing of typical messages. Message size restrictions override message priority, meaning that even high priority messages are delayed if they exceed the size restrictions.

4. Click **Save**, then click **Close** to return to the main Admin console window.

If a user's message is not sent out of the domain because of this restriction, the user receives an email message providing the following information:

`Delivery disallowed - Transfer limit is` *`nn`* `MB`

However, the message is delivered to recipients in the sender's own domain.

There are additional ways to restrict the size of messages that users can send, as described in "Restricting the Size of Messages That Users Can Send" on page 125.

Configuring a Routing Domain

As you create each new domain in your GroupWise system, you link it to another domain. You can view and modify the links between domains using the Link Configuration Tool. See Chapter 10, "Managing the Links between Domains and Post Offices," on page 101.

As an alternative to configuring individual links between individual domains throughout your GroupWise system, you can establish a system of one or more routing domains. Domains must connect to the routing domains with TCP/IP links.

A routing domain can serve as a hub in the following situations:

- Messages that are otherwise undeliverable can be automatically sent to a single routing domain. This routing domain can be set up to perform DNS lookups and route messages out across the Internet.
- All messages from a domain can be automatically routed through another domain, regardless of the final destination of the messages. This provides additional control of message flow through your GroupWise system.

You can set up routing domains on two levels:

- "Selecting a System Default Routing Domain" on page 231
- "Selecting a Specific Routing Domain for an Individual Domain" on page 232

Selecting a System Default Routing Domain

You can establish a single default routing domain for your entire GroupWise system. This provides a centralized routing point for all messages. It takes precedence over specific links established when domains were created or links modified with the Link Configuration Tool.

To set up a system default routing domain:

1. In the GroupWise Admin console, click **System > System Preferences**.
2. On the **General** tab, locate the **Routing Options** section.
3. In the **Default Routing Domain** field, browse to and select the domain you want to serve as the default routing domain for your entire GroupWise system.
4. If you want all GroupWise messages to pass through the default routing domain regardless of the destination of the message, select **Force All Messages to This Domain**.

   or

If you want only undeliverable GroupWise messages to be routed to the default routing domain, deselect **Force All Messages to This Domain**.

If you do not force all messages to the system default routing domain, then you have the option of allowing selected MTAs to provide routing domain services in addition to the system default routing domain.

5. Select **MTAs Send Directly to Other GroupWise Systems** if you want all MTAs in your GroupWise system to perform DNS lookups and route messages out across the Internet.

   or

   Deselect **MTAs Send Directly to Other GroupWise Systems** if you want to individually designate which MTAs should perform DNS lookups and route messages out across the Internet.
6. Click **OK** to save the routing options you have specified for the system default routing domain.

Selecting a Specific Routing Domain for an Individual Domain

As long as you are not forcing all messages to the system default routing domain, you can override the system default routing information for an individual domain.

1. In the GroupWise Admin console, browse to and click the MTA.
2. Click the **General** tab, and locate the **Routing Options** section.

   System default routing information displays if it has been set up. See "Selecting a System Default Routing Domain" on page 231.
3. Select **Override** next to the default information you want to change for the selected domain.
4. Set the routing options as needed for the selected domain.
5. Click **Save**, then click **Close** to return to the main Admin console window.

MTA Console: You can check routing information on the Configuration page under the **General Settings** heading.

Configuring User Synchronization

You can configure the MTA to synchronize user information in the GroupWise Address Book with user information in an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory. You can also configure the MTA to allow the Outlook Client and Mac Mail to access the System Address Book by enabling an LDAP server.

Configuring LDAP User Synchronization

When you import GroupWise users from an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory, you can select an MTA to synchronize updated user information from the LDAP directory into GroupWise. User synchronization is typically configured when the LDAP directory is established, but you can set it up or reconfigure it later as needed.

For instructions, see "Configuring User Synchronization for an LDAP Directory" on page 80.

Configuring Exchange Address Book Synchronization

Starting in GroupWise 2012 SP2, the MTA can perform address book synchronization between GroupWise and Exchange.

Exchange address book synchronization requires its own license. If you enable Exchange address book synchronization, your GroupWise system might be subject to additional licensing fees. We invite you to contact your Micro Focus representative, reseller, or partner to learn more about this feature or for pricing and licensing information.

For setup instructions, see the *GroupWise/Exchange Coexistence Guide*.

Configuring the LDAP Server Capabilities

The LDAP Server provides a read-only interface into the GroupWise System Address Book. This allows lookups and queries via LDAP for the Outlook client. You can also use the LDAP server to provision GroupWise Mobility Service users. For more information, see Selecting the User Source for Your Mobility System in the *GroupWise Mobility Service 18 Installation Guide*.

1 In the GroupWise Admin Console, browse to and click the MTA.

2 Click the **LDAP** tab.

3 Select **Enable LDAP**.

4 (Optional) Specify a Port number.

   The default port for non-SSL is 389. The default port for SSL is 636.

5 (Optional) Enable SSL.

   If SSL is enabled after the port is changed, the port will be reset to the default.

6 (Conditional) If SSL is enabled, you can select to **Use the MTA Certificate and Key** or upload your own certificate and key file.

   6a In the **SSL Certificate File** field, click the **Browse** icon.

   6b Click **Upload Local File to Server**, then click **Browse**.

   6c Browse to and select the SSL certificate file on your local workstation.

   You can use certificate files in the PEM, PFX, CRT, B64, or CER format.

   6d Click **Upload** to upload the certificate file into the GroupWise `certificates` folder on the server where the POA is running.

   6e Click **OK**.

   6f In the **SSL Key File** field, browse to, select, and upload the private key file, then click **OK**.

   6g Click **Save** to save the SSL certificate and key files.

7 (Optional) Select **Set Password** to specify and confirm a password for the key file.

To setup the Outlook client to connect to the GroupWise System Address Book through the LDAP server, see Configuring GroupWise Address Lookup in the Microsoft Outlook Client in the *GroupWise Mobility Service 18 Administration Guide*.

Known Limitations

- You cannot run a **Contains** search.
- Any filter beginning with a “*” will fail.
- In Outlook, autocomplete will only work if you manually add the users as a contact. This is an Outlook limitation.

* The only attributes available for search are **Email**, **First name**, **Last Name**, and **Display name**.
* You cannot currently use a GroupWise created certificate for SSL.
* You must restart the gwadminservice on the MTA server after enabling the LDAP server capabilities for it to be active.

23 Managing the MTA

Setting Up the MTA Console

The web-based MTA console is set up automatically when you create a new domain. You can optionally protect the MTA console with a user name and password, or use an SSL connection between your web browser and the MTA.

1. In the GroupWise Admin console, browse to and click the MTA.
2. Click the **Agent Settings** tab and locate the **HTTP** section.
3. (Conditional) If you want to use an SSL connection for the MTA console, which provides optimum security, select **Enabled** or **Required** in the **HTTP SSL** drop-down list.
   - **Enabled:** If the MTA is configured with a valid SSL certificate, the MTA console uses SSL. If a valid SSL certificate is not available, the MTA still provides the MTA console, but without a secure SSL connection.
   - **Required:** The MTA does not support the MTA console unless a valid SSL certificate has been provided.

   For additional instructions about using SSL connections, see "Server Certificates and SSL Encryption" on page 695.
4. If you want to limit access to the MTA console, fill in the **HTTP User Name** and **HTTP Password** fields.

   Unless you are using SSL, do not use a user name that is synchronized from an LDAP directory (such as NetIQ eDirectory or Microsoft Active Directory). This is because the information passes over the non-secure connection between your web browser and the agent. If you are using SSL, the user name is encrypted and therefore secure.
5. Click **Save**, then click **Close** to return to the main Admin console window.
6. Continue with Accessing the MTA Console.

Corresponding Startup Switches: You can also use the --httpport, --httpuser, and --httppassword startup switches in the MTA startup file to enable the MTA console. In addition, you can use the --httprefresh switch to control how often the MTA refreshes the information provided to your web browser.

Accessing the MTA Console

1. In the GroupWise Admin console, browse to and click the MTA.
2. On the **General** tab, click **Launch MTA Console**.

   In the MTA console, you can change some MTA log settings for the current MTA session. You can also stop and start some specific MTA threads.

TIP: To access the MTA console directly from your web browser, provide the URL where the MTA is located by supplying the network address and port number. For example:

```
http://mta_server_address:7100
http://mta_server_address:7180
```

To view the MTA console, you can specify either the message transfer port or the HTTP port.

IMPORTANT: In order to control the MTA from the MTA console, you must set up authentication for the MTA console, as described in "Setting Up the MTA Console" on page 235.

Changing MTA Configuration Settings

On the MTA console menu, click **Configuration**. Online help on the Configuration page helps you interpret the configuration information being displayed.

Click the **Event Log Settings** heading to change the MTA log settings for the current MTA session.

Controlling Links to Other Locations

On the MTA console menu, click **Links**. Select one or more locations, then click **Suspend** or **Resume** as needed.

24 Monitoring the MTA

By monitoring the MTA, you can determine whether or not its current configuration is meeting the needs of your GroupWise system. You have a variety of resources to help you monitor the operation of the MTA:

Using the MTA Console

The MTA console enables you to monitor the MTA from any location where you have access to a web browser and the Internet. This provides substantially more flexible access than the MTA server console, which can only be accessed from the server where the MTA is running.

The MTA console provides several pages of information to help you monitor the performance of the MTA. The title bar at the top of the MTA console displays the name of the MTA and its domain. Below the title bar appears the MTA console menu that lists the pages of information available in the MTA console. Online help throughout the MTA console helps you interpret the information being displayed and use the links provided.

Monitoring MTA Status

When you first access the MTA console, the Status page is displayed. Online help throughout the MTA console helps you interpret the information being displayed and use the links provided.

Click the **Router** link to display details about the MTA routing queue (`gwinprog`). You can quickly determine how many messages are awaiting processing, how large they are, and how long they have been waiting in the routing queue.

Click a closed location to display its holding queue to see how many messages are waiting for transfer.

Monitoring the Routing Queue

On the MTA console menu, click **Status**, then click **Router** to display the contents of the routing queue. Typically, no message files are waiting unless the MTA is down or backlogged.

You can click any queue to view the message files it contains.

Monitoring Links

On the MTA console menu, click **Links** to monitor the direct links between the MTA and other locations.

Click a location to view its holding queue. Click **View Link Configuration** to determine the address of each location and access the agent consoles of other domains and of post offices that belong to the local domain. Click **View TCP/IP Connections** to view incoming and outgoing TCP/IP links. Click **View Gateways** to restrict the list to just gateways.

Tracking Messages

Before you can track messages at the MTA console, you must enable message logging for MTAs throughout your system. See "Enabling MTA Message Logging" on page 228. When you enable MTA message logging, the MTA stores data about GroupWise message traffic as it processes messages. The stored data is then available for use from the MTA console.

To track a specific message, have the sender check the Sent Item Properties for the message in the GroupWise client. The **Mail Envelope Properties** field displays the message ID of the message; for example, 3AD5EDEB.31D : 3 : 12763. To track all messages sent by a particular user, make a note of the user's GroupWise user ID.

On the MTA console menu, click **Message Tracking**.

Fill in *one* of the fields, depending on what you want to track, then click **Submit**. The results of the search are displayed on a separate page which can be printed.

Using MTA Log Files

Error messages and other information about MTA functioning are written to log files and can be displayed in the POA console. Log files can provide a wealth of information for resolving problems with MTA functioning or message flow. This section covers the following subjects to help you get the most from MTA log files:

Locating MTA Log Files

The default location of the MTA log files varies by platform:

Linux:	`/var/log/novell/groupwise/`*`domain_name`*`.mta`
Windows:	`mslocal` subfolder in the folder specified by the --work switch

You can change the location where the MTA creates its log files, as described in Configuring MTA Log Settings and Switches.

Configuring MTA Log Settings and Switches

When installing or troubleshooting the MTA, a logging level of Verbose can be useful. However, when the MTA is running smoothly, you can set the logging level down to Normal to conserve disk space occupied by log files.

1. In the GroupWise Admin console, browse to and click the MTA.
2. Click the **Log Settings** tab.
3. Set the desired settings for logging.

   Log File Path: Browse to and select the folder where you want this MTA to store its log files.

   Logging Level: Select the amount of data displayed on the MTA agent console and written to the MTA log file.

   - **Off:** Turns off disk logging and sets the logging level for the MTA to its default. Logging information is still displayed on the MTA agent console.
   - **Normal:** Displays only the essential information suitable for a smoothly running MTA.

- **Verbose:** Displays the essential information, plus additional information that can be helpful for troubleshooting.
- **Diagnostic:** Turns on **Extensive Logging Options** and **SOAP Logging Options** on the MTA console Log Settings page.

Maximum Log File Age: Specifies how many days to keep MTA log files on disk. The default is 30 days.

Maximum Log Disk Space: Sets the maximum amount of disk space for all MTA log files. When the specified disk space is consumed, the MTA deletes existing log files, starting with the oldest. The default is 100 MB. The maximum allowable setting is 1000 (1 GB).

Corresponding Startup Switches: You can also use the --log, --loglevel, --logdays, --logmax, and --logdiskoff switches in the MTA startup file to configure logging.

Viewing and Searching MTA Log Files

You can view the contents of the MTA log file in the MTA console.

1. In the MTA console, click **Log Files**.
2. To view a log file, select the log file, then click **View Events**.
3. To select specific types of MTA processing to search for, select one or more of the following types:
   - **Message Logging (MLG):** The message logging threads write information into the message log file if message logging has been turned on. See "Enabling MTA Message Logging" on page 228.
   - **Event Logging (LOG):** The event logging thread writes information into the event log files that you can search on this page. See "Using MTA Log Files" on page 238.
   - **Dispatcher (DIS):** The dispatcher thread starts other MTA threads as needed to meet the demands being put on the MTA at any given time.
   - **Message Transfer (MTP):** The message transfer threads communicate with other MTAs and with POAs in the local domain to transfer messages to domains and post offices to which the local MTA is linked by way of TCP/IP.
   - **Routing (RTR):** The router threads process messages in the routing queue and prepare them for transfer to the next hop in the link path to their destinations. See "Optimizing the Routing Queue" on page 244.
   - **Admin (ADM):** The admin thread updates the domain database (`wpdomain.db`) whenever administrative information changes.
   - **Scanner (SCA):** The scanner threads check for incoming messages when UNC or mapped links are in use.
4. To search for a specific string, select the log files to search, specify the string in the **Events Containing** field, then click **View Events**.

   TIP: To search all log files, select **Select All**.

   ---
5. To create a new log file, click **Cycle Log**.

Interpreting MTA Log File Information

On startup, the MTA records the MTA settings currently in effect. Thereafter, it logs events that take place, including errors.

Because the MTA consists of multiple threads, you might find it useful to retrieve the log file into an editor and sort it on the thread ID that follows the date and time information. Sorting groups all messages together for the same MTA thread.

Using GroupWise Monitor

GroupWise Monitor is a monitoring and management tool that allows you to monitor GroupWise agents from any location where you are connected to the Internet and have access to a web browser. In addition, GroupWise Monitor can notify you when agent problems arise.

For installation and setup instructions, see "Setting Up GroupWise Monitor" in the *GroupWise 18 Installation Guide*. For usage instructions, see Part XVII, "Monitor," on page 637.

Using Micro Focus Remote Manager

When GroupWise agents are running on Micro Focus Open Enterprise Server (OES), you can use Micro Focus Remote Manager to monitor them. For more information, see the *Micro Focus Remote Manager Administration Guide*.

Using an SNMP Management Console

You can monitor the GroupWise agents from SNMP management and monitoring programs. When properly configured, the GroupWise agents send SNMP traps to network management consoles for display along with other SNMP monitored programs.

Although the GroupWise agents are SNMP-enabled by default, the server where the GroupWise agents are installed must be properly configured to support SNMP, and the agents must also be properly configured. To set up SNMP services, complete the following tasks:

Setting Up SNMP Services for the MTA

Select the instructions for the platform where the MTA runs:

- "Linux: Setting Up SNMP Services for the MTA" on page 240
- "Windows: Setting Up SNMP Services for the MTA" on page 241

Linux: Setting Up SNMP Services for the MTA

The Linux GroupWise agents are compatible with NET-SNMP. An older version of SNMP called UCD-SNMP cannot be used with the Linux GroupWise agents. NET-SNMP comes with OES, but it does not come with SLES. If you are using SLES, you must update to NET-SNMP in order to use SNMP to monitor the Linux GroupWise agents.

1. Ensure you are logged in as root.
2. If NET-SNMP is not already set up on your Linux server, use the following command to configure SNMP:

```
snmpconf -g basic_setup
```

The `snmpconf` command creates the `snmpd.conf` file in one of the following folders, depending on your version of Linux:

```
/usr/share/snmp
/usr/local/share/snmp
~/.snmp
```

3 Locate the `snmpd.conf` file on your Linux server.

4 In a text editor, open the `snmpd.conf` file and add or uncomment the following lines:

```
dlmod Gwsnmp /opt/novell/groupwise/agents/lib/libgwsnmp.so
export LD_LIBRARY_PATH=/opt/novell/groupwise/agents/lib
export MIBDIRS=/usr/share/snmp/mibs:/opt/novell/groupwise/agents/mibs
export MIBS=ALL
```

5 Save the `snmpd.conf` file and exit the text editor.

6 Restart the SNMP daemon (snmpd) to put the changes into effect.

IMPORTANT: Ensure that the SNMP daemon always starts before the POA starts.

Skip to "Copying and Compiling the MTA MIB File" on page 241.

Windows: Setting Up SNMP Services for the MTA

SNMP support is automatically installed along with the GroupWise agents. SNMP support is provided for up to instances of each GroupWise agent on the same Windows server. Upon startup, each instance of a GroupWise agent is dynamically assigned a row in its SNMP table. View the contents of the agent MIB for a description of the SNMP variables in the table.

On some versions of Windows Server, the SNMP Service is not included during the initial operating system installation. The SNMP Service can be added either before or after the GroupWise agents are installed on the Windows server.

Copying and Compiling the MTA MIB File

An SNMP-enabled GroupWise agent returns information contained in a Management Information Base (MIB). The MIB is an ASCII data structure that defines the information gathered. It also defines the properties that can be monitored and managed on the SNMP-enabled GroupWise agent.

Before you can monitor an SNMP-enabled GroupWise agent, you must compile the agent MIB file using your SNMP management program. GroupWise agent MIB files are located in the `/agents/mibs` folder in your GroupWise software installation.

The MIB file contains all the Trap, Set, and Get variables used for communication between the GroupWise agent and the SNMP management console. The Trap variables provide warnings that point to current and potential problems. The Set variables allow you to configure portions of the application while it is still running. The Get variables display the current status of different processes of the application.

1 Copy the agent MIB file to the location required by your SNMP management program.

2 Compile or import the agent MIB file as required by your SNMP management program.

Continue with Configuring the MTA for SNMP Monitoring.

Configuring the MTA for SNMP Monitoring

In order for SNMP monitoring programs to monitor the a GroupWise agent, the GroupWise agent must be configured with an SNMP community string.

1. In the GroupWise Admin console, browse to and click the GroupWise agent object.
2. Click the **Agent Settings** tab, then locate the **SNMP Community "Get" String** field.
3. Provide your system SNMP community "Get" string, then click **OK**.
4. Configure the SNMP Service with the same community "Get" string.
5. Restart the GroupWise agent.

   The GroupWise agent should now be visible to your SNMP monitoring program.

Receiving Notifications of Agent Problems

If you want to be notified with an email message whenever GroupWise agents encounter a critical error, you can add yourself to the list of users to notify.

1. In the GroupWise Admin console, browse to and click a domain.
2. Click the **General** tab.
3. In the **Notify User** field, browse to and select a GroupWise user or group.

   A domain can have a single notification user, or you can create a group to function as notification users.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Corresponding Startup Switches: By default, the MTA generates error mail if an administrator has been assigned for the domain. Error mail can be turned off using the --noerrormail switch.

TIP: Another way to receive email notification of MTA problems is to use GroupWise Monitor. See "Configuring Email Notification" on page 645.

Using MTA Message Logging

For extremely detailed monitoring of message flow, you can configure the MTA to gather a variety of statistics. See "Enabling MTA Message Logging" on page 228.

25 Optimizing the MTA

You can adjust how the MTA functions to optimize its performance. Before attempting optimization, you should run the MTA long enough to observe its efficiency and its impact on other network applications running on the same server. See Chapter 24, “Monitoring the MTA,” on page 237.

Also, remember that optimizing your network hardware and operating system can make a difference in MTA performance.

Optimizing TCP/IP Links

Using startup switches in the MTA startup file, you can fine-tune the performance of TCP/IP links.

Adjusting the Number of MTA TCP/IP Connections

When using TCP/IP links between domains, you can control the number of inbound connections the MTA can establish for receiving messages from POAs and GWIAs in the same domain and from MTAs and GWIAs in other domains in your GroupWise system.

Use the --tcpinbound switch in the MTA startup file to increase the maximum number of inbound connections the MTA can establish from the default of 40 to whatever setting meets the needs of your system. There is no maximum setting.

If the MTA is receiving more requests than it can accept, the sending MTAs must wait until a connection becomes available, which slows down message transfer. Each connection requires only about 20 KB. For example, if you configure the MTA to accept 600 connections, it would require approximately 12 MB of RAM. Although there is no maximum setting for inbound connections, this setting is adequate to handle very heavy usage. Use lower settings to conserve RAM or for lighter usage.

MTA Console: You can check the maximum number of TCP/IP connections that the MTA can start on the Configuration page under the **TCP/IP Settings** heading.

Adjusting the MTA Wait Intervals for Slow TCP/IP Connections

When using TCP/IP links, you can control how long the MTA waits for responses.

By default, the MTA waits 5 seconds for a response when trying to contact another MTA or a POA across a TCP/IP link. If no response is received from the other MTA or the POA, the sending MTA tries again three more times. If all four attempts fail, the MTA reports an error, then waits 10 minutes before it tries again.

When the MTA attempts to send messages to another MTA or a POA across a TCP/IP link, the sending MTA tries for 20 seconds before reporting an error.

On some networks, these wait intervals might not be sufficient, and the MTA might report an error when, by waiting longer, the needed connection or data transfer could take place.

Use the --tcpwaitconnect switch in the MTA startup file to increase the number of seconds the MTA waits for a response from another MTA or a POA across a TCP/IP link.

Use the --tcpwaitdata switch in the MTA startup file to increase the number of seconds the MTA attempts to send messages to another MTA or a POA across a TCP/IP link.

MTA Console: You can check the current wait intervals on the Configuration page under the **TCP/IP Settings** heading.

Optimizing the Routing Queue

Using startup switches in the MTA startup file, you can fine-turn MTA processing in of the routing queue. When the MTA starts, it starts one or more router threads to process its routing queue (`gwinprog`). As messages arrive in the routing queue, it starts additional routers as needed, within parameters you can set.

MTA Console: You can view the current contents of the routing queue from the Status page. Click **Router** under the **Queue Information** heading.

Adjusting the Maximum Number of Active Router Threads

By default, the MTA continues to start additional router threads to processes messages in the routing queue as long as message traffic demands it, until as many as 16 router threads are running. Use the --maxrouters switch in the MTA startup file to control the number of router threads the MTA can start.

Set --maxrouters to a lower number to conserve resources and keep the MTA from starting more than the specified maximum number of router threads.

Adjusting the Maximum Number of Idle Router Threads

By default, after the MTA starts a router thread, it keeps it running, up to the maximum number specified by the --maxrouters switch. In a system where short bursts of heavy message traffic are followed by extended lulls, idle router threads could be consuming resources that would be better used by other processes. Use the --maxidlerouters switch in the MTA startup file to determine how many idle router threads are allowed to remain running. The default is 16 idle router threads.

Set --maxidlerouters to a lower number if you want the MTA to terminate idle router threads more quickly. Set --maxidlerouters to a higher number if you want the MTA to keep more idle router threads ready to process incoming message traffic.

Adjusting MTA Polling of Closed Locations

When a location becomes closed (unavailable), the MTA waits before attempting to recontact that location. If the MTA waits only a short period of time, the MTA can waste time and create network traffic by trying to reestablish a connection with a closed location. On the other hand, you do not want the MTA to ignore an available location by waiting too long.

By default, the MTA waits 600 seconds (10 minutes) between its attempts to contact a closed location. You can adjust the time interval the MTA waits to meet the needs of your GroupWise system.

1. In the GroupWise Admin console, browse to and click the MTA.
2. Click the **Agent Settings** tab.

3 Decrease the number of seconds in the **Attach Retry** field if you want the MTA to try to contact closed locations more often.

   or

   Increase the number of seconds in the **Attach Retry** field if you want the MTA to try to contact closed locations less often.

4 Click **Save**, then click **Close** to return to the main Admin console window.

For a TCP/IP link, a location is considered open if the MTA receives a response from the receiving agent within the currently configured wait intervals. See "Adjusting the MTA Wait Intervals for Slow TCP/IP Connections" on page 243. Otherwise, the location is considered closed.

For a mapped or UNC link, a location is considered open if the MTA can perform the following actions:

- Create a temporary folder in the MTA input queue (*domain*\wpcsin and *post_office*\wpcsin folders)
- Create a temporary file in that new folder
- Delete the temporary file
- Delete the temporary folder

26 Using MTA Startup Switches

You can override settings provided in the GroupWise Admin console by using startup switches in the MTA startup file. The default location for the MTA startup file is in the domain folder.

When you create a domain and install the MTA, an initial MTA startup file is created. It is named using the first 8 characters of the domain name with a `.mta` extension. This initial startup file includes the --home startup switch set to the location of the domain folder.

Startup switches specified on the command line override those in the startup file. Startup switches in the startup file override corresponding settings in the GroupWise Admin console. You can view the MTA startup file from the Configuration page of the MTA console.

The table below summarizes MTA startup switches and how they correspond to configuration settings in the GroupWise Admin console.

Switch starts with: a b c d e f g h i j k l m n o p q r s t u v w x y z

Linux MTA	Windows MTA	GroupWise Admin Console Settings
@file_name	*@file_name*	N/A
--activelog	/activelog	N/A
--adminport	/adminport	N/A
--certfile	/certfile	**Certificate File**
--cluster	/cluster	N/A
--cyhi	/cyhi	**Scan High**
--cylo	/cylo	**Scan Cycle**
--defaultroutingdomain	/defaultroutingdomain	**Default Routing Domain**
--dhparm	/dhparm	N/A
--fast0	/fast0	**Use 2nd High Priority Scanner**
--fast4	/fast4	**Use 2nd Mail Priority Scanner**
--help	/help	N/A
--home	/home	N/A
--httppassword	/httppassword	**HTTP Password**
--httpport	/httpport	**HTTP Port**
--httprefresh	/httprefresh	N/A
--httpssl	/httpssl	**HTTP**
--httpuser	/httpuser	**HTTP User Name**
--ip	/ip	**TCP/IP Address**
--keyfile	/keyfile	**SSL Key File**

Linux MTA	Windows MTA	GroupWise Admin Console Settings
--keypassword	/keypassword	SSL Key File Password
--language	/language	N/A
--log	/log	Log File Path
--logdays	/logdays	Max Log File Age
--logdiskoff	/logdiskoff	Logging Level
--loglevel	/loglevel	Logging Level
--logmax	/logmax	Max Log Disk Space
--maxidlerouters	/maxidlerouters	N/A
--maxrouters	/maxrouters	N/A
--messagelogdays	/messagelogdays	Delete Reports After
--messagelogmaxsize	/messagelogmaxsize	N/A
--messagelogpath	/messagelogpath	Message Log File Path
--messagelogsettings	/messagelogsettings	Message Logging Level
--msgtranssl	/msgtranssl	Message Transfer SSL
--noada	/noada	N/A
--nodns	/nodns	N/A
--noerrormail	/noerrormail	N/A
--nondssync	/nondssync	N/A
--norecover	/norecover	N/A
--nosnmp	/nosnmp	N/A
--show	N/A	N/A
--sslciphersuite	/sslciphersuite	N/A
--ssloption	/ssloption	N/A
--tcpinbound	/tcpinbound	N/A
--tcpport	/tcpport	Network Address
--tcpwaitconnect	/tcpwaitconnect	N/A
--tcpwaitdata	/tcpwaitdata	N/A
--vsnoadm	/vsnoadm	N/A
--work	/work	N/A

@startup_file_name

Specifies the location of the MTA startup file. The MTA startup file is created in the domain folder and is named after the domain, with a `.mta` extension. The startup file includes the --home switch.

	Linux MTA	Windows MTA
Syntax:	@[/*dir*/]*file*	@[*drive*:][*dir*\\]*file*
Example:	./gwmta @../share/lnxdom.mta	gwmta.exe @provo2.mta gwmta.exe @d:\agt\provo2.mta

--activelog

Displays the active log window rather than the alert box when the MTA starts with a user interface.

	Linux MTA	Windows MTA
Syntax:	--activelog	/activelog

--adminport

Specifies the port number used for the MTA to communicate with the GroupWise Admin Service. The default port number is 9710.

	Linux POA	Windows POA
Syntax:	--adminport *port_number*	/adminport-*port_number*
Example:	--adminport 9720	/adminport-9720

--certfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the MTA and other programs. See "Securing the Domain with SSL Connections to the MTA" on page 229.

	Linux MTA	Windows MTA
Syntax:	--certfile-/*dir*/*file*	/certfile-[*drive*:]*dir**file* /certfile-*svr**sharename**dir**file*
Example:	--certfile /certs/gw.crt	/certfile-\ssl\gw.crt /certfile-m:\ssl\gw.crt /certfile-\\\\server2\c\ssl\gw.crt

See also --keyfile and --keypassword.

--cluster

Informs the MTA that it is running in a cluster. A clustered MTA automatically binds to the IP address configured for the MTA object even if the **Bind Exclusively to TCP/IP Address** option is not selected on the MTA **Agent Settings** tab in the GroupWise Admin console. This prevents unintended connections to other IP addresses, such as the loopback address or the node's physical IP address. For information about clustering the MTA, see the *GroupWise 18 Interoperability Guide*.

	Linux MTA	Windows MTA
Syntax:	--cluster	/cluster

See also /ip.

--cyhi

Sets the number of seconds in the scan cycle that the MTA uses to scan its priority 0-1 input queues. The default is 5 seconds.

	Linux MTA	Windows MTA
Syntax:	--cyhi-*seconds*	/cyhi-*seconds*
Example:	--cyhi 3	/cyhi-3

See also --cylo.

--cylo

Sets the number of seconds in the scan cycle that the MTA uses to scan its priority 2-7 input queues. The default is 15 seconds.

	Linux MTA	Windows MTA
Syntax:	--cylo-*seconds*	/cylo-*seconds*
Example:	--cylo 10	/cylo-10

See also --cyhi.

--defaultroutingdomain

Identifies the domain name in your GroupWise system to which all MTAs should send messages when they cannot resolve the available routing information to a specific *user.post_office.domain* GroupWise address. See "Configuring a Routing Domain" on page 231.

	Linux MTA	Windows MTA
Syntax:	--defaultroutingdomain *domain*	/defaultroutingdomain-*domain*

	Linux MTA	Windows MTA
Example:	--defaultroutingdomain inethub	/defaultroutingdomain-inethub

--dhparm

Specifies a Diffie-Hellman cipher parameters file used for SSL/TLS to replace the default parameters set by GroupWise. GroupWise uses default Diffie-Hellman parameters of 2048 bits to generate the DH key. A valid DH parameter is in PEM format.

	Linux MTA	Windows MTA
Syntax:	--dhparm *directory/pemfile*	/dhparm *directory/pemfile*
Example:	--dhparm /var/tmp/dh.pem	/dhparm C:\temp\dh.pem

--fast0

Causes the MTA to monitor and process the priority 0 and 1 subfolders independently with separate scanner threads, rather than in sequence with the same scanner thread.

	Linux MTA	Windows MTA
Syntax:	--fast0	/fast0

See also --fast4.

--fast4

Causes the MTA to monitor and process the priority 2 and 3 subfolders with a separate scanner thread from the priority 4 through 7 subfolders.

	Linux MTA	Windows MTA
Syntax:	--fast4	/fast4

See also --fast0.

--help

Displays the MTA startup switch Help information. When this switch is used, the MTA does not start.

	Linux MTA	Windows MTA
Syntax:	--help or --?	/help or /?
Example:	./gwmta --help	gwmta.exe /help

--home

Specifies the domain folder, where the MTA can access the domain database (`wpdomain.db`). There is no default location. You must use this switch in order to start the MTA.

	Linux MTA	Windows MTA
Syntax:	--home /*dir*	/home-[*drive*:]*dir* /home-*svr**sharename**dir*
Example:	--home /gwsystem/provo2	/home-\provo2 /home-m:\provo2 home-\\\\server2\c\mail\provo2

If you specify a UNC path with the --home switch when you run the MTA as a Windows service, you must configure the MTA service to run under a specific Windows user account. If you specify a local folder or a mapped drive, you can configure the MTA service to run under the local system account. However, running under the Administrator account is highly recommended.

--httppassword

Specifies the password for the MTA to prompt for before allowing MTA status information to be displayed in your web browser. Do not use an existing LDAP directory password because the information passes over the non-secure connection between your web browser and the MTA. See "Using the MTA Console" on page 237.

	Linux MTA	Windows MTA
Syntax:	--httppassword *unique_password*	/httppassword-*unique_password*
Example:	--httppassword AgentWatch	/httppassword-AgentWatch

See also /httpuser, /httpport, /httprefresh, and /httpssl.

--httpport

Sets the HTTP port number used for the MTA to communicate with your web browser. The default is 7180; the setting must be unique. See "Using the MTA Console" on page 237.

	Linux MTA	Windows MTA
Syntax:	--httpport *port_number*	/httpport-*port_number*
Example:	--httpport 3802	/httpport-3803

See also --httpuser, --httppassword, --httprefresh, and --httpssl.

--httprefresh

Specifies the rate at which the MTA refreshes the status information in your web browser. The default is 60 seconds. See "Using the MTA Console" on page 237.

	Linux MTA	Windows MTA
Syntax:	--httprefresh *seconds*	/httprefresh-*seconds*
Example:	--httprefresh 90	/httprefresh-120

See also --httpuser, --httppassword, --httpport, and --httpssl.

--httpssl

Enables secure SSL communication between the MTA and the MTA console displayed in your web browser. See "Securing the Domain with SSL Connections to the MTA" on page 229.

	Linux MTA	Windows MTA
Syntax:	--httpssl	/httpssl

See also --certfile, --keyfile, and --keypassword.

--httpuser

Specifies the user name for the MTA to prompt for before allowing MTA status information to be displayed in your web browser. Providing a user name is optional. Do not use an existing LDAP directory user name because the information passes over the non-secure connection between your web browser and the MTA. See "Using the MTA Console" on page 237.

	Linux MTA	Windows MTA
Syntax:	--httpuser *unique_name*	/httpuser-*unique_name*
Example:	--httpuser GWWebCon	/httpuser-GWWebCon

See also --httppassword, --httpport, and --httprefresh.

--ip

Binds the MTA to a specific IP address when the server where it runs uses multiple IP addresses. The specified IP address is associated with both ports used by the MTA (message transfer and HTTP) Without the --ip switch, the MTA binds to all available IP addresses. See "Binding the MTA to a Specific IP Address" on page 228.

	Linux MTA	Windows MTA
Syntax:	--ip *IP_address* --ip "*full_dns_name*"	/ip-*IP_address* /ip-"*full_dns_name*"

	Linux MTA	Windows MTA
Example:	--ip 172.16.5.18 --ip “mtasvr.provo.novell.com”	/ip-172.16.5.18 /ip-”mtasvr.provo.novell.com”

--keyfile

Specifies the full path to the private file used to provide secure SSL communication between the MTA and other programs. See “Securing the Domain with SSL Connections to the MTA” on page 229.

	Linux MTA	Windows MTA
Syntax:	--keyfile /*dir*/*file*	/keyfile-[*drive*:]*dir**file* /keyfile-*svr**sharename**dir**file*
Example:	--keyfile /ssl/gw.key	/keyfile-\ssl\gw.key /keyfile-m:\ssl\gw.key /keyfile-\\\\server2\c\ssl\gw.key

See also --certfile and --keypassword.

--keypassword

Specifies the password used to encrypt the private SSL key file when it was created. See “Securing the Domain with SSL Connections to the MTA” on page 229.

	Linux MTA	Windows MTA
Syntax:	--keypassword *password*	/keypassword-*password*
Example:	--keypassword gwssl	/keypassword-gwssl

See also --certfile and --keyfile.

--language

Specifies the language to run the MTA in, using a two-letter language code as listed below. You must install the MTA in the selected language in order for the MTA to display in the selected language.

The initial default is the language used in the domain. If that language has not been installed, the next default is the language used by the operating system. If that language has not been installed, the final default is English. You only need to use this switch if you need to override these defaults.

	Linux MTA	Windows MTA
Syntax:	--language *code*	/language-*code*
Example:	--language de	/language-fr

Contact your local Micro Focus sales office for information about language availability.

See Chapter 7, "Multilingual GroupWise Systems," on page 85 for a list of language codes.

--log

Specifies the folder where the MTA will store its log files. The default location varies by platform.

Linux: `/var/log/novell/groupwise/`*`domain_name`*`.mta`

Windows: `mslocal` subfolder in the folder specified by the --work switch

For more information, see "Using MTA Log Files" on page 238.

	Linux MTA	Windows MTA
Syntax:	--log /*dir*	/log-[*drive*:]*dir* /log-*svr**sharename**dir*
Example:	--log /gwsystem/logs	/log-\agt\log /log-m:\agt\log /log-\\\\server2\c\mail\agt\log

You typically find multiple log files in the specified folder. The first four characters represent the date. The next three characters identify the agent. A three-digit extension allows for multiple log files created on the same day. For example, a log file named `0518mta.001` indicates that it is an MTA log file, created on May 18. If you restarted the MTA on the same day, a new log file is started, named `0518mta.002`.

See also --loglevel, --logdiskoff, --logdays, and --logmax.

--logdays

Sets the number of days you want MTA log files to remain on disk before being automatically deleted. The default log file age is 30 days. The valid range is from 1 to 350 days. See "Using MTA Log Files" on page 238.

	Linux MTA	Windows MTA
Syntax:	--logdays *days*	/logdays-*days*
Example:	--logdays 45	/logdays-60

See also --log, --loglevel, --logdiskoff, and --logmax.

--logdiskoff

Turns off disk logging for the MTA so no information about the functioning of the MTA is stored on disk. The default is for logging to be turned on. See "Using MTA Log Files" on page 238.

	Linux MTA	Windows MTA
Syntax:	--logdiskoff	/logdiskoff

See also --loglevel.

--loglevel

Controls the amount of information logged by the MTA. Logged information is displayed in the log message box and written to the MTA log file during the current agent session. The default is Normal, which displays only the essential information suitable for a smoothly running MTA. Use Verbose to display the essential information, plus additional information helpful for troubleshooting. Verbose logging does not degrade MTA performance, but log files saved to disk consume more disk space when verbose logging is in use. See "Using MTA Log Files" on page 238.

	Linux MTA	Windows MTA
Syntax:	--loglevel *level*	/loglevel-*level*
Example:	--loglevel verbose	/loglevel-verbose

See also --log, --logdiskoff, --logdays, and --logmax.

--logmax

Sets the maximum amount of disk space for all MTA log files. When the specified disk space is consumed, the MTA deletes existing log files, starting with the oldest. The default is 102400 KB (100 MB) of disk space for all MTA log files. The maximum allowable setting is 102400000 (1 GB). Specify 0 (zero) for unlimited disk space. See "Using MTA Log Files" on page 238.

	Linux MTA	Windows MTA
Syntax:	--logmax *kilobytes*	/logmax-*kilobytes*
Example:	--logmax 130000	/logmax-160000

See also --log, --loglevel, --logdiskoff, and --logdays.

--maxidlerouters

Specifies the maximum number of idle router threads the MTA can keep running. The default is 16; valid values range from 1 to 16. See "Optimizing the Routing Queue" on page 244.

	Linux MTA	Windows MTA
Syntax:	--maxidlerouters *threads*	/maxidlerouters-*threads*
Example:	--maxidlerouters 10	/maxidlerouters-12

See also --maxrouters.

--maxrouters

Specifies the maximum number of router threads the MTA can start. The default is 16; valid values range from 1 to 16. See “Optimizing the Routing Queue” on page 244.

	Linux MTA	Windows MTA
Syntax:	--maxrouters *threads*	/maxrouters-*threads*
Example:	--maxrouters 12	/maxrouters-14

See also --maxidlerouters.

--messagelogdays

Sets the number of days you want MTA message log files to remain on disk before being automatically deleted. The default is 30 days. See “Configuring MTA Log Settings and Switches” on page 238.

	Linux MTA	Windows MTA
Syntax:	--messagelogdays *days*	/messagelogdays-*days*
Example:	--messagelogdays 45	/messagelogdays-60

See also --messagelogsettings, --messagelogpath, and --messagelogmaxsize.

--messagelogmaxsize

Sets the maximum size for MTA message log files. The default is 102400 KB (100 MB). The maximum allowable setting is 102400000 (1 GB). See “Enabling MTA Message Logging” on page 228.

	Linux MTA	Windows MTA
Syntax:	--messagelogmaxsize *kilobytes*	/messagelogmaxsize-*kilobytes*
Example:	--messagelogmaxsize 130000	/messagelogmaxsize-160000

See also --messagelogsettings, --messagelogpath, and --messagelogdays.

--messagelogpath

Specifies the folder for the MTA message log. The default location is `mlocal\msglog`. See “Enabling MTA Message Logging” on page 228.

	Linux MTA	Windows MTA
Syntax:	--messagelogpath /*dir*	/messagelogpath-[*drive*:]*dir* /messagelogpath-*svr**sharename**dir*

	Linux MTA	Windows MTA
Example:	--messagelogpath /gwsys/logs	/messagelogpath-\mta\log /messagelogpath-m:\mta\log /messagelogpath-\\svr2\c\mail\mta\log

See also --messagelogsettings, --messagelogdays, and --messagelogmaxsize.

--messagelogsettings

Enables MTA message logging. See "Enabling MTA Message Logging" on page 228.

	Linux MTA	Windows MTA
Syntax:	--messagelogsettings *codes*	/messagelogsettings-*codes*
Example:	--messagelogsettings e	/messagelogsettings-e

See also --messagelogpath, --messagelogdays, and --messagelogmaxsize.

--msgtranssl

Enables secure SSL communication between the MTA and the POAs in its domain. See "Securing the Domain with SSL Connections to the MTA" on page 229.

	Linux MTA	Windows MTA
Syntax:	--msgtranssl	/msgtranssl

See also --certfile, --keyfile, and --keypassword.

--noada

Disables the MTA admin thread.

	Linux MTA	Windows MTA
Syntax:	--noada	/noada

Historical Note: In GroupWise 5.2 and earlier, a separate agent, the Administration Agent (ADA), handled the functions now consolidated into the MTA admin thread. Hence the switch name, --noada.

--nodns

Disables DNS lookups for the MTA.

	Linux MTA	Windows MTA
Syntax:	--nodns	/nodns

--noerrormail

Prevents error files from being sent to the GroupWise administrator. The default is for error mail to be sent to the administrator. See “Receiving Notifications of Agent Problems” on page 242.

	Linux MTA	Windows MTA
Syntax:	--noerrormail	/noerrormail

--nondssync

Disables LDAP user synchronization.

	Linux MTA	Windows MTA
Syntax:	--nondssync	N/A

--norecover

Disables automatic database recovery. The default is for automatic database recovery to be turned on. If the MTA detects a problem with the domain database (`wpdomain.db`) when automatic database recovery has been turned off, the MTA notifies the administrator, but it does not recover the problem database. See Chapter 42, “Maintaining Domain and Post Office Databases,” on page 395.

	Linux MTA	Windows MTA
Syntax:	--norecover	/norecover

--nosnmp

Disables SNMP for the MTA. The default is to have SNMP enabled. See “Using an SNMP Management Console” on page 240.

	Linux MTA	Windows MTA
Syntax:	--nosnmp	/nosnmp

--show

Starts the MTA with a server console user interface.

By default, no user interface is provided for the agents on Linux. An agent that runs with a user interface cannot be managed in the GroupWise Admin console.

The --show startup switch can be used on the command line or in the `gwha.conf` file used by the GroupWise High Availability Service. It cannot be placed in the agent startup file.

	Linux MTA	Windows MTA
Syntax:	--show	N/A

The --show switch cannot be used in the MTA startup file. However, if you want the MTA to start with a user interface when you run the `grpwise` script or when the server reboots, you can configure the GroupWise High Availability service (gwha) to accomplish this, as described in "Editing the gwha.conf File to Enable SSL and Customize Agent Management (Optional)" in the *GroupWise 18 Installation Guide*.

--sslciphersuite

Sets the SSL cipher suites used by the Archive Agent, the Messaging Agent, and Messenger clients. The cipher list must be in OpenSSL format. For more information on OpenSSL format, see Cipher List Format (https://www.openssl.org/docs/apps/ciphers.html#CIPHER-LIST-FORMAT)

	Linux MTA	Windows MTA
Syntax:	--sslciphersuite *"setting"*	/sslciphersuite-*"setting*"
Example:	--sslciphersuite "HIGH:!AECDH:!EXP:@STRENGTH"	/sslciphersuite-"HIGH:!AECDH:!EXP:@STRENGTH"

--ssloption

Specify a specific SSL protocol to disable. By specifying SSL_OP_NO_TLSv1, GroupWise will disable TLSv1 support. Specify additional options by adding the SSL key work separated by a comma.

	Linux MTA	Windows MTA
Syntax:	--ssloption *SSL_protocol*	/ssloption *SSL_protocol*
Example:	--ssloption SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1	/ssloption SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1

--tcpinbound

Sets the maximum number of inbound TCP/IP connections for the MTA from POAs and GWIAs belonging to the domain and from MTAs and GWIAs in other domains in your GroupWise system. The default is 40. There is no maximum number of outbound connections. The only limit on the MTA for outbound connections is available resources. See "Adjusting the Number of MTA TCP/IP Connections" on page 243.

	Linux MTA	Windows MTA
Syntax:	--tcpinbound *number*	/tcpinbound-*number*

	Linux MTA	Windows MTA
Example:	--tcpinbound 60	/tcpinbound-70

--tcpport

Sets the TCP port number on which the MTA listens for incoming messages from other MTAs, POAs, and GWIAs. The default is 7100.

	Linux MTA	Windows MTA
Syntax:	--tcpport *port_number*	/tcpport-*port_number*
Example:	--tcpport 7200	/tcpport-7200

--tcpwaitconnect

Sets the maximum number of seconds the MTA waits for a connection to another MTA. The default is 5. See "Adjusting the MTA Wait Intervals for Slow TCP/IP Connections" on page 243.

	Linux MTA	Windows MTA
Syntax:	--tcpwaitconnect *seconds*	/tcpwaitconnect-*seconds*
Example:	--tcpwaitconnect 10	/tcpwaitconnect-10

See also --tcpwaitdata.

--tcpwaitdata

Sets the maximum number of seconds the MTA attempts to send data over a TCP/IP connection to another MTA. The default is 20. See "Adjusting the MTA Wait Intervals for Slow TCP/IP Connections" on page 243.

	Linux MTA	Windows MTA
Syntax:	--tcpwaitdata *seconds*	/tcpwaitdata-*seconds*
Example:	--tcpwaitdata 30	/tcpwaitdata-30

See also --tcpwaitconnect.

--vsnoadm

Prevents GroupWise administration messages from being processed by an integrated virus scanner. Because administration messages are created within your GroupWise system, they are not likely to contain viruses. In a GroupWise system with a large amount of administrative activity (adding users, deleting users, etc.), skipping the virus scanning of administrative messages can speed up processing of users' email messages.

	Linux MTA	Windows MTA
Syntax:	--vsnoadm	/vsnoadm

--work

Specifies the folder where the MTA creates its local working folder (`mslocal`). The default is the domain folder. However, if the domain is located on a different server from where the MTA will run, use a local folder so the MTA cannot lose its connection to its `mslocal` folder.

	Linux MTA	Windows MTA
Syntax:	--work /*dir*	/work-[*drive*:]*dir* /work-*svr**sharename**dir*
Example:	--work /gwmta	/work-\gwmta /work-m:\gwmta /work-\\\\server2\c\mail\gwmta

VI Internet Agent

For a complete list of port numbers used by the GWIA, see "Internet Agent Port Numbers" on page 728.

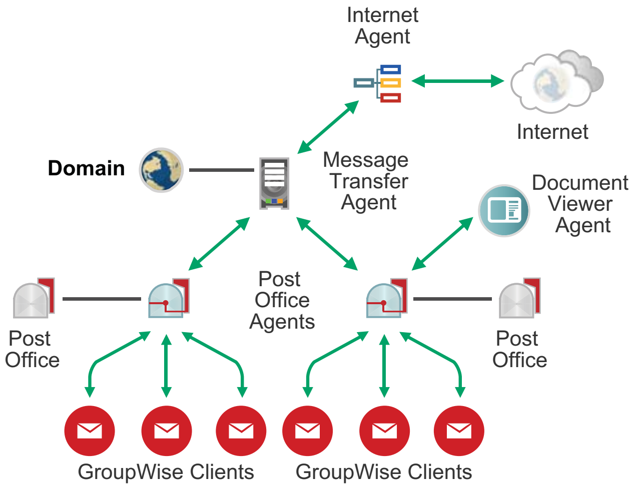
For detailed Linux-specific GWIA information, see Appendix C, "Linux Basics for GroupWise Administration," on page 735.

27 Understanding Message Transfer to and from the Internet

The GWIA in Your GroupWise System

The Internet Agent (GWIA) provides communication between GroupWise users and users of other messaging systems who send email across the Internet. The GWIA picks up inbound email messages from the Internet, converts them from RFC-822 or MIME format to the GroupWise message format, and then passes the converted messages to the GroupWise Message Transfer Agent (MTA).

For outgoing messages to the Internet, the MTA passes the messages to the GWIA, which then converts the messages to Internet messaging format, and then sends them to the designated Internet addresses.



GWIA Representation in the GroupWise Admin Console

In the GroupWise Admin console, GWIAs are listed on the Overview page, under the domains that they belong to.

Services Provided by the GWIA

- "SMTP/MIME Service" on page 266
- "POP3 Service" on page 266
- "IMAP4 Service" on page 267
- "iCal and iMip Services" on page 267
- "Secure Connections via SSL" on page 267

* “Access Control” on page 267
* “Multiple Threading” on page 267
* “SNMP-Compliant” on page 267

SMTP/MIME Service

The SMTP/MIME service in the GWIA enables you to send and receive email with standard encoding on attachments, international character sets, and multipart messages. Multimedia email with images, sound, and video can also be exchanged. The service also includes these additional features:

* **SMTP Dial-Up Service:** The GWIA includes SMTP dial-up functionality. This can be useful when your system does not meet the requirements of a dedicated Internet connection, or when you prefer not to have a permanent Internet connection. With the SMTP dial-up feature, you can establish a schedule to periodically check the message store without maintaining a permanent link.
* **Flexible Addressing:** The GWIA offers full GroupWise addressing support, including system groups, nicknames, and individual users.

  The GWIA also takes advantage of GroupWise Internet addressing, which allows inbound messages addressed in a variety of formats to be delivered to GW users. These formats include:

  ```
  User_Name@Internet_domain_name
  User_Name.PostOffice@Internet_domain_name
  Last_Name.First_Name@Internet_domain_name
  First_Name.Last_Name@Internet_domain_name
  First_Initial_Last_Name@Internet_domain_name
  ```
* **Internet Users in the Address Book:** Internet users can be added to the GroupWise Address Book so users won’t have to remember long Internet addresses.
* **Real-Time Blacklists:** Organizations such as SpamCop provide lists of IP addresses that are known to be open relay hosts or spam hosts. You can use the real-time blacklists provided by such sites to protect your users from offensive spam.
* **Spam Protection:** Anti-spam services use different indicators to mark potential spam. One might use a string of asterisks; the more asterisks, the greater the likelihood that the message is spam. Another might use a numerical value; the higher the number, the greater the likelihood that the message is spam. You can configure the GWIA to recognize as spam whatever indicators your anti-spam service uses and flag such messages for processing by the client Junk Mail Handling feature.
* **Accounting:** The accounting feature provides inbound and outbound tracking of messages passing through the GWIA. This lets administrators track how the GWIA is being used. GroupWise Monitor includes a Gateway Accounting report that organizes information gathered in GWIA accounting files into a format that is visually easy to read.
* **DNS Name Resolution:** The GWIA can access a DNS server directly to resolve host names to IP addresses, or it can rely on a relay host to perform the name resolution.
* **Connect to Other GroupWise Systems Through the Internet:** With passthrough addressing, you can connect to other GroupWise systems anywhere on the Internet and have access to all of the GroupWise features. The Internet simply becomes a mail transport medium for GroupWise.

POP3 Service

The Post Office Protocol 3 (POP3) service in the GWIA allows you to download messages from your GroupWise post office to a POP3 client application such as a web browser’s email program or a Telnet application. The GWIA acts as the POP3 server, providing a TCP connection between the

user's GroupWise post office and a POP3 client. Accessing the GroupWise post office via the GWIA's POP3 server capability, users can retrieve their email messages and manage them through user name login options.

IMAP4 Service

The GWIA supports the Internet Messaging Access Protocol 4 (IMAP4). As an IMAP4 server, the GWIA allows IMAP4-compliant email clients to read and manipulate GroupWise messages.

iCal and iMip Services

The GWIA supports iCalendar (iCal), the Internet Calendaring and Scheduling core object specification (RFC 2445), and iMIP, the iCalendar Message-based Interoperability Protocol (RFC 2447). When a GroupWise user sends an appointment to an external Internet user, the GWIA converts the appointment into an iMIP message that can be read and accepted, declined, or canceled in compatible email systems such as Microsoft Exchange and Lotus Notes. GroupWise users can also receive and accept, decline, or cancel appointments from users of these email systems. Accept/decline notifications are also exchanged between systems. In addition, tasks to an from users in other email systems can be marked Completed.

Secure Connections via SSL

The GWIA supports the use of SSL for its connections to SMTP hosts, POP3 clients, IMAP4 clients, and GWIA console.

Access Control

The GWIA includes security capabilities called Access Control that allow administrators to control user access to all services (SMTP/MIME, POP3, and IMAP4). Access Control can help you reduce costs and provide added security.

With the SMTP/MIME service, Access Control can be used to block messages being sent to or received from specific host or IP addresses.

Multiple Threading

Multiple threading enables more than one send or receive process to be running concurrently. You can configure the number of threads to enhance the speed and performance of the GWIA. The number of threads are set separately for the SMTP/MIME service, POP3 service, and IMAP4 service.

SNMP-Compliant

The GWIA can be managed by any SNMP-compliant network manager.

28 Configuring the GWIA

For GWIA system requirements, see “Internet Agent Functional Requirements” in the *GroupWise 18 Installation Guide*. The GWIA can optionally be installed as part of creating a new domain. For installation instructions, see “GWIA Configuration” and “Adding a Secondary Domain” in the *GroupWise 18 Installation Guide*. The GWIA can also be added to a domain after it has been created. For setup instructions, see “Creating a New GWIA in the GroupWise Admin Console” on page 269.

As your GroupWise system grows and evolves, you might need to modify your GWIA configuration to meet the changing needs of your system.

Creating a New GWIA in the GroupWise Admin Console

The initial GWIA object is automatically created when you choose to install the GWIA as part of creating a new domain. You can later add a GWIA to a domain where you did not initially choose to install one. Typically, you do not need more than one GWIA in a domain, but if you want to customize the processing of multiple GWIAs, you can do so. For example, you might want a GWIA that is dedicated to servicing IMAP clients, because IMAP processing has high overhead.

1. In the GroupWise Admin console, connect to the domain where you want to install the GWIA.
2. Click **Internet Agents > New**.
3. Specify a unique name for the GWIA object.
4. Specify the fully qualified Internet hostname of the server where the GWIA runs, such as `gwia.example.com`, or the name of the "A record" in your DNS table that associates the hostname with the server's IP address.
5. Set the time zone, language, and platform as needed, then click **OK**.

Creating a new GWIA object accomplishes the following additional tasks:

- Creates the *`domain`*`/wpgate/gwia` subfolder.
- Creates the `gwia.cfg` file with the --home switch set to the `gwia` subfolder.
- On Linux, adds the new GWIA to the `gwha.conf` file.
- On Windows, configures the new GWIA as a Windows service.
- Starts the new GWIA.

If you want additional GWIAs that are not associated with domains where post offices and mailboxes are located, you can set up a new domain server specifically to house one or more additional GWIAs.

Configuring the GWIA in the GroupWise Admin Console

The advantage to configuring the GWIA in the GroupWise Admin console, as opposed to using startup switches in a GWIA startup file, is that the GWIA configuration settings can be easily edited from any location where the Admin console is available.

1. In the GroupWise Admin console, browse to and click the GWIA.
2. For information about each tab and field, click **Help**.

   The context-sensitive help topics link to the related sections of this guide, where you can determine which GWIA startup switch corresponds to each GWIA setting in the GroupWise Admin console. Some GWIA configuration can be done only using a startup file. For more information, see in Chapter 34, "Using GWIA Startup Switches," on page 319.

Configuring an Alternate GWIA for a Domain

You can configure an alternate GWIA for a domain, so that if the domain's primary GWIA goes down, the MTA can fail over to another GWIA in your GroupWise system until the primary GWIA is up and running again. This feature is especially useful in large GroupWise systems with multiple GWIAs that handle a lot of Internet messages.

1. In the GroupWise Admin console, browse to and click the Domain.
2. Click the **Internet Addressing** tab and locate the **Internet Agent for Outbound SMTP/MIME Messages** section.
3. Click **Override**.
4. In the **Alternate Internet Agent for Outbound SMTP/MIME Messages** field, select a GWIA as an alternate for this domain.
5. Click **Save**, then click **Close** to return to the main Admin console window.

The MTA always tries to transfer outbound Internet messages to the primary GWIA first, so after an outage the primary GWIA automatically resumes its normal processing for the domain.

Binding the GWIA to a Specific IP Address

By default, the GWIA binds to all IP addresses when the server where it runs uses multiple IP addresses. The each IP address is associated with all ports used by the agent.

To use an exclusive bind to a one specific IP address:

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click **Agent Settings** and locate the **Network Address** section.
3. Select **Bind Exclusively to TCP/IP Address**.
4. Click **Save**, then click **Close** to return to the main Admin console window.

You can use the /ip startup switch in the GWIA startup file to establish an exclusive bind to the specified IP address. If you have used this switch in the GWIA startup file, remove it to turn off the exclusive bind.

Securing Internet Access with SSL Connections to the GWIA

The GWIA can use the SSL (Secure Socket Layer) protocol to enable secure connections to other SMTP hosts, POP/IMAP clients, and the GWIA console. For the GWIA to do so, you must ensure that it has access to a server certificate file and that you have configured the connection types (SMTP, POP, IMAP, HTTP) you want secured through SSL.

For background information about SSL and how to set it up on your system, see "Server Certificates and SSL Encryption" on page 695.

To configure the GWIA to require SSL:

1 In the GroupWise Admin console, browse to and click the GWIA.

2 On the **GroupWise** tab, click **SSL Settings**.

3 (Conditional) If you need to generate a new self-signed certificate for the GWIA:

   The GroupWise Admin Service generates a certificate signing request (CSR) and a private key file, and then sends them to the GroupWise certificate authority (CA) on the primary domain. The CA issues the requested certificate, which is then returned to the local server.

   3a Click **Generate Certificate**.

   3b Specify and confirm the password for the private key file for the new SSL certificate, then click **OK**.

   The newly created SSL certificate and private key files display on the **SSL Settings** tab.

   3c Click **Save** to save the SSL certificate and key files.

4 (Conditional) If you already have an SSL certificate and key file for the GWIA:

   4a In the **SSL Certificate File** field, click the **Browse** icon.

   4b Click **Upload Local File to Server**, then click **Browse**.

   4c Browse to and select the SSL certificate file on your local workstation.

   You can use certificate files in the PEM, PFX, CRT, B64, or CER format.

   4d Click **Upload** to upload the certificate file into the GroupWise `certificates` folder on the server where the GWIA is running.

   4e Click **OK**.

   4f In the **SSL Key File** field, browse to, select, and upload the private key file, then click **OK**.

   4g Click **Save** to save the SSL certificate and key files.

5 To enable or require SSL connections for the GWIA, click **Agent Settings** on the **GroupWise** tab.

6 Enable or require SSL connections between the GWIA and the MTA, select **Enabled** or **Required** in the **Message Transfer SSL** drop-down list.

   The MTA must also use SSL for the connection to be secure. See "Securing the Domain with SSL Connections to the MTA" on page 229.

   IMPORTANT: To prevent closed links between agents, select **Enabled** when you are initially configuring agents for SSL. Select **Required** for tighter security only after all agents are successfully using SSL.

   ---

7 (Optional) Select **Enabled** or **Required** in the **SSL** drop-down list for other protocols as needed.

8 Click **Save**, then click **Close** to return to the main Admin console window.

Deleting a GWIA

1. In the GroupWise Admin console, browse to and click the GWIA to delete.
2. Click **Delete**.
3. (Optional) Select **Delete Database Files**.
4. Click **Yes** to delete the GWIA and, optionally, the files and most of the folders located in the GWIA's `wpgate` subfolder.

   The queue folders (`wpcsin` and `wpcsout`) are not deleted.
5. (Optional) Manually delete GWIA's `wpgate` subfolder, including the `wpcsin` and `wpcsout` subfolders.

29 Managing Internet Domains, Addressing, and Access

When you created your GroupWise system, you set up the initial Internet domain name. You can establish additional Internet domain names for your GroupWise system as needed. As you manage the Internet domain names for your GroupWise system, you do the following tasks:

- Define additional Internet domain names for your GroupWise system. You can have one or more domain names (for example, `novell.com`, `gw.novell.com`, and `support.novell.com`).
- Set up the default Internet address format for use when displaying user addresses in the GroupWise Address Book and in sent messages. There are six formats that can be assigned at the system, domain, post office, or user level. In addition, there is a free-form format that can be used at the user level.
- Designate the address formats that can be used to address messages to your GroupWise users. There are five possible formats to choose from. You can allow all five formats, or only one.
- Specify the default GWIA to be used when sending messages from your GroupWise system to the Internet. This becomes your system's default GWIA for outbound messages sent from all domains; however, if you have multiple GWIAs, you can override this setting by assigning GWIAs at the domain level.

The following sections help you plan and set up Internet addressing:

Planning GWIAs Used for Outbound Messages

Each domain in your GroupWise system must be assigned a GWIA for outbound messages. A domain's assigned GWIA handles all outbound messages sent by the domain's users.

If your GroupWise system includes only one GWIA, that GWIA must be assigned to all domains and is used for all outbound messages.

If your GroupWise system includes multiple GWIAs, you must decide which GWIA you want to be responsible for outbound messages for each domain. You must select one GWIA as your system's default GWIA, but you can override the default at each domain.

Planning Internet Domain Names

You must associate at least one Internet domain (such as `novell.com`, `gw.novell.com`, or `support.novell.com`) with your GroupWise system. These Internet domains need to exist in the domain name service (DNS).

After you have associated Internet domains with your GroupWise system, all users in your system can be addressed using any of the domains (for example, `jsmith@novell.com`, `jsmith@gw.novell.com`, and `jsmith@support.novell.com`). The addresses can be used both internally and externally.

Preferred Internet Domain Name

You must assign each GroupWise user a preferred Internet domain. GroupWise uses the preferred Internet domain name when constructing the email addresses that are displayed in the GroupWise Address Book and in the **To** field of sent messages.

To make this process easier, GroupWise lets you assign a preferred Internet domain to be used as the default for your GroupWise system (for example, `novell.com`). The system's preferred Internet domain is applied to all users in your GroupWise system. However, you can override the system's preferred Internet domain at the domain, post office, or user level, meaning that different users within your GroupWise system can be assigned different preferred Internet domains. For example, users in one domain can be assigned `gw.novell.com` as their preferred Internet domain while users in another domain are assigned support.novell.com.

Understanding Internet Addressing Formats

Preferred Address Format

You must choose a preferred address format for your GroupWise users. GroupWise uses the preferred address format, along with the preferred Internet domain, to construct the email addresses that are published in the GroupWise Address Book and in the **To** and **From** fields of sent items.

GroupWise supports the following address formats:

user_name.post_office.domain@internet_domain_name
user_name.post_office@internet_domain_name
user_name@internet_domain_name
firstname.lastname@internet_domain_name
lastname.firstname@internet_domain_name
firstinital lastname@internet_domain_name

As with the preferred Internet domain, you must assign a preferred address format to be used as the default for your GroupWise system. The system's preferred address format is applied to all users in your GroupWise system. However, you can override the system's preferred address format at the domain, post office, and user/resource level.

The following sections explain some of the advantages and disadvantages of each address format:

- "user_name.post_office.domain@internet_domain_name" on page 274
- "user_name.post_office@internet_domain_name" on page 275
- "user_name@internet_domain_name" on page 275
- "firstname.lastname@internet_domain_name" on page 275
- "lastname.firstname@internet_domain_name" on page 276
- "firstinitial lastname@internet_domain_name" on page 276

user_name.post_office.domain@internet_domain_name

Advantages

- Reliable format. GroupWise guarantees that each address is unique.
- Identical user names can be used in different post offices.

Disadvantages

- Addresses tend to be long and hard to remember.
- Addresses might change over time as users are moved from one post office to another.

user_name.post_office@internet_domain_name

Advantages

- Guarantees uniqueness if all your post offices have unique names.
- Identical user names can be placed in different post offices.

Disadvantages

- Addresses tend to be long and hard to remember.
- Addresses might change over time as users are moved from one post office to another.

user_name@internet_domain_name

Advantages

- Addresses are short and easy to remember.
- Backward-compatible with previous versions of GroupWise. (Users won't need to update their business cards.)
- Addresses do not change as users are moved.

Disadvantages

- When you first enable this address format, you might have duplicate user names in your GroupWise system. However, in the future, the GroupWise Admin console prevents you from creating duplicate user names within the same Internet domain name. The same user name can be used in different Internet domains without problem.

firstname.lastname@internet_domain_name

Advantages

- Addresses are intuitive and easy to remember.
- Addresses do not change as users are moved.

Disadvantages

- When you first enable this address format, you might have duplicate first and last names in your GroupWise system. However, in the future, the GroupWise Admin console prevents you from creating users with the same first and last names within the same Internet domain name. The same first name and last name combination can be used in different Internet domains without problem.
- The probability of conflicts increases if any user's first and last names match any GroupWise domain or post office name, if any two users have the same first and last names, or if any two users have the opposite first and last names (such as James Dean and Dean James).

lastname.firstname@internet_domain_name

Advantages

- Addresses are intuitive and easy to remember.
- Addresses do not change as users are moved.

Disadvantages

- When you first enable this address format, you might have duplicate first and last names in your GroupWise system. However, in the future, the GroupWise Admin console prevents you from creating users with the same first and last names within the same Internet domain name. The same last name and first name combination can be used in different Internet domains without a problem.
- The probability of conflicts increases if any user's first and last names match any GroupWise domain or post office name, if any two users have the same first and last names, or if any two users have the opposite first and last names (such as James Dean and Dean James).

firstinitial lastname@internet_domain_name

Advantages

- Addresses are intuitive and easy to remember.
- Addresses do not change as users are moved.

Disadvantages

- When you first enable this address format, you might have duplicate first initial and last names in your GroupWise system. However, in the future, the GroupWise Admin console prevents you from creating users with the same first initials and last names within the same Internet domain name. The same first initial and last name combination can be used in different Internet domains without problem
- The probability of conflicts increases when using first initials instead of complete first names.

Allowed Address Formats

The preferred Internet domain and preferred address format apply to user addresses as displayed in the GroupWise Address Book or in the address displayed on sent messages.

The allowed address formats, on the other hand, determine which address formats are accepted by the GWIA. There are five possible allowed formats:

user_name.post_office@internet_domain_name

user_name@internet_domain_name

firstname.lastname@internet_domain_name

lastname.firstname@internet_domain_name

firstinital lastname@internet_domain_name

If you select all five formats, the GWIA accepts messages addressed to users in any of the formats. For example, John Peterson would receive messages sent using any of the following addresses:

`jpeterson.research@novell.com`

```
jpeterson@novell.com
john.peterson@novell.com
peterson.john@novell.com
jpeterson@novell.com
```

You must designate the allowed address formats to be used as the default formats for your GroupWise system. The system's allowed address formats are applied to all users in your GroupWise system. However, you can override the system's allowed address formats at the domain, post office, and user/resource level.

For example, assume you have two John Petersons with user names of jpeterson and japeterson. The `user_name.post_office` and `user_name` address formats do not cause message delivery problems, but the `firstname.lastname`, `lastname.firstname`, and `firstinitial lastname` address formats do. To overcome this problem, you could disallow the three problem formats for these users at the user level.

Configuring Internet Addressing

After yo have decided how you want to handle email addresses in your GroupWise system, implementing the customizations is an easy task.

Adding Internet Domain Names

You can have as many Internet domain names for your GroupWise system as needed. Each Internet domain name must be valid with your Internet service provider.

1 In the GroupWise Admin console, click **System > Internet Addressing**.

  The first Internet domain name was established when your GroupWise system was created.

2 Click **New** to add another Internet domain name for your GroupWise system.

3 Specify the new Internet domain name, then click **OK**.

  The new Internet domain name is added to your GroupWise system.

4 (Optional) To make the new Internet domain name the preferred Internet domain name for your GroupWise system, click the check box beside the Internet domain name, then click **Set Preferred**.

  The preferred Internet domain name is used in addresses published in the GroupWise Address Book and in the **To** field of sent messages

5 Click **OK** to close the list of Internet domain names.

Establishing Default GWIAs for Domains

The default GWIA for outbound messages for your GroupWise system is the first GWIA that is installed. It might be installed in the primary domain or in a secondary domain. When you install more GWIAs, you can change the default GWIA for your GroupWise system by using **System > Internet Addressing > Internet Domains > Internet Agent for Outbound SMTP/MIME Messages**.

You can override the system default Internet domain name separately for each domain.

1 In the GroupWise Admin console, browse to and client the name of a domain.

2 Click the **Internet Addressing** tab.

3 Click **Override**, then select the Internet domain name for this domain.

4 (Optional) Select **For Incoming Mail, Recipients Are Known Exclusively by This Internet Domain Name** to restrict the email addresses that are accepted for users in this domain.

5 Click **Save**, then click **Close**.

Changing the Preferred and Allowed Address Formats for Your GroupWise System

The initial preferred and allowed address formats for your GroupWise system are established when you created your GroupWise system. You can change them at any time.

1 In the GroupWise Admin console, click **System > Internet Addressing,** then click the **Address Formats** tab.

2 Change the address formats as needed then click **Save**.

   If your users are associated with User objects in an LDAP directory, and if you changed the preferred address format, you are prompted to update the email addresses for the affected users in the LDAP directory. We recommend that you allow this update. However, performing it for a large segment of your GroupWise system might take a while.

3 Click **Yes** to confirm, then click **Close** when the process is completed.

Overriding Internet Addressing

All domains, post offices, and users/groups/resources in your GroupWise system inherit the Internet addressing defaults (GWIA for outbound messages, preferred Internet domain name, preferred address format, and allowed address formats). However, if desired, you can override these defaults for individual objects.

1 In the GroupWise Admin console, browse to and click a domain, a post office, a user, a group, or a resource.

2 Click the **Internet Addressing** tab.

   At the domain level, you can override all Internet addressing defaults assigned to your GroupWise system.

   At the post office level, you can override the preferred Internet domain name, the preferred address format, and the allowed address formats that the post office has inherited from its domain. You cannot override the GWIA that is assigned to handle outbound messages from the domain.

   At the user, group, and resource level, you can override the preferred Internet domain, the preferred address format, and the allowed address formats that the user/resource has inherited from its post office. You cannot override the GWIA that is assigned to handle outbound messages from the domain.

3 Select **Override** for the settings that you want to change, adjust the settings as needed, then click **Save**.

   If you changed the preferred address format, and if the users are associated with User objects in an LDAP directory, you are prompted to update the Internet email address. The Internet email address is the address that is returned in response to LDAP queries to the LDAP directory. We recommend that you allow this update. However, performing it for a large segment of your GroupWise system might take a while.

4 Click **Save**, then click **Close** to return to the main Admin console window.

Setting a Preferred Email ID

At the user, group, and resource level, the preferred address format can be completely overridden by explicitly defining the user portion of the address format (`user@Internet_domain_name`). The user/group/resource portion can include any RFC-compliant characters.

For example, if you have selected `First Name.Last Name@Internet domain name` as your system's preferred address format and you have two John Petersons, each on a different post office in your system, you would end up two users having the same address (`John.Peterson@novell.com`). You could use this field to differentiate them by including their middle initials in their address (`John.S.Peterson@novell.com` and `John.A.Peterson@novell.com`).

You can use the same email ID for more than one user in your GroupWise system, if each user is in a different Internet domain. Rather than requiring that each email ID be unique in your GroupWise system, each combination of email ID and Internet domain must be unique. This provides more flexibility for handling the situation where two people have the same name.

1. In the GroupWise Admin console, browse to and click the name of a User, a Group, or a Resource, then click **Internet Addressing**.
2. In the **Preferred Email ID** section, click **Override**, then specify the unique email address for the user/group/resource.

   Use any RFC-compliant characters.
3. Click **Save**, then click **Close**.

Managing Internet Access

After you have configured the Internet services that you want the GWIA to provide in your GroupWise system, you need to take control of the information that flows in and out between your GroupWise system and the Internet.

Controlling User Access to the Internet

You can use the GroupWise GWIA's Access Control feature to configure a user's ability to send and receive SMTP/MIME messages to and from Internet recipients and to access his or her mailbox from POP3 or IMAP4 email clients. In addition to enabling or disabling a user's access to features, you can configure specific settings for the features. For example, for outgoing SMTP/MIME messages, you can limit the size of the messages or the sites to which they can be sent. By default, there are no limitations.

Access Control can be implemented at a user, group, post office, or domain level.

Choose from the following information to learn how to set up and use Access Control.

- "Classes of Service" on page 280
- "Creating a Class of Service" on page 281
- "Managing Classes of Service" on page 284
- "Testing Access Control Settings" on page 284
- "Maintaining the Access Control Database" on page 284

Classes of Service

A class of service is a specifically defined configuration of GWIA privileges. A class of service controls the following types of access activities:

- Whether SMTP/MIME messages are allowed to transfer to and from the Internet
- Whether SMTP/MIME messages are allowed to transfer to and from specific domains on the Internet
- The maximum size of SMTP/MIME messages that can transfer to and from the Internet
- Whether SMTP/MIME messages generated by GroupWise rules are allowed to transfer to the Internet
- Whether IMAP4 clients are allowed to access the GroupWise system
- Whether POP3 clients are allowed to access the GroupWise system, and if allowed, how messages to and from POP3 clients are managed by the GroupWise system

The default class of service, which all users belong to, allows incoming and outgoing SMTP/MIME messages, and allows POP3 and IMAP4 access. You can control user access, at an individual, group, post office, or domain level, by creating different classes of service and adding the appropriate members to the classes. For example, you could create a class of service that limits the size of SMTP/MIME messages for a selected individual, group, post office, or domain.

Because you can assign membership at the user, group, post office, and domain level, it is possible that a single user can be a member of multiple classes of service. This conflict is resolved hierarchically, as shown in the following table:

Membership assigned to a user through a...	Overrides membership assigned to the user through the...
domain	• default class of service
post office	• default class of service • domain
group	• default class of service • domain • post office
user	• default class of service • domain • post office

If a user's membership in two classes of service is based upon the same level of membership (for example, both through individual user membership), the class that applies is the one that allows the most privileges.

IMPORTANT: The GWIA uses the message size limit set for the default class of service as the maximum incoming message size for your GroupWise system. Therefore, you should set the message size for the default class of service to accommodate the largest message that you want to allow into your GroupWise system. As needed, you can then create other classes of service with smaller message size limits to restrict the size of incoming messages for selected users, groups, post offices, or domains. Methods for restricting message size within your GroupWise system are described in "Restricting the Size of Messages That Users Can Send" on page 125.

Attachments to incoming SMTP messages are included in the `mime.822` file, in addition to being attached to the message. Therefore, attachments contribute twice to the size of the overall message. Take this account when determining the maximum incoming message size for your GroupWise system.

Creating a Class of Service

1. In the GroupWise Admin console, connect to the domain of the GWIA.
2. Browse to and click the GWIA.
3. Click the **Access Control** tab, then click **Settings**.
4. Click **New** to display the Create New Class of Service dialog box.
5. Type a name for the class, then click **OK** to display the Edit Class of Service dialog box.
6. On the **SMTP Incoming** tab, choose from the following options:

   Inherit Access: Members of this class of service inherit their SMTP Incoming access from a class of service assigned at a higher level. For example, a post office inherits the domain's access. If the domain is not a member of a class of service, the post office inherits the default class of service.

   Allow Incoming Messages: Enable members of the class of service to receive email messages through the GWIA. You can use the **Exceptions** option to prevent messages from specific Internet sites.

   Prevent Incoming Messages: Prevent email messages coming from the Internet. You can use the **Exceptions** option to allow messages from specific Internet sites.

   NOTE: If a member of the class of service to allow or prevent has an alias, you must also add the member's alias to the class of service. Ongoing use of aliases is not recommended.

   Prevent Messages Larger Than: This option is available only if you chose **Allow Incoming Messages** or **Prevent Incoming Messages**. In the case of **Prevent Incoming Messages**, this option only applies to messages received from Internet sites listed in the **Allow Messages From** list.

   If you want to set a size limit on incoming messages, select the limit.

   Internet messages that exceed the limit are not delivered. The sender receives an email message indicating that the message is undeliverable and including the following explanation:

   `Message exceeds maximum allowed size`

   IMPORTANT: If you have also set a message size limit for your MTAs, ensure that the MTA message size limit is equal to or greater than the GWIA message size limit. For more information, see "Restricting Message Size between Domains" on page 230.

   Exceptions: This option is available only if you chose **Allow Incoming Messages** or **Prevent Incoming Messages**.

   Prevent Messages From: If you chose to allow incoming messages but you want to prevent messages from specific Internet sites (IP addresses or DNS hostnames), add the sites to the **Prevent Messages From** list.

   Allow Messages From: Conversely, if you chose to prevent incoming messages but you want to allow messages from specific Internet sites (IP addresses or DNS hostnames), add the sites to the **Allow Messages From** list.

   If you want to allow messages where the user name is blank, add Blank-Sender-User-ID to the **Allow Messages From** list.

7 Click **SMTP Outgoing**, then choose from the following options:

Inherit Access: Members of this class of service inherit their **SMTP Outgoing** access from a class of service assigned at a higher level. For example, a post office inherits the domain's access. If the domain is not a member of a class of service, the post office inherits the default class of service.

Allow Outgoing Messages: Allow members of the class of service to send email messages over the Internet. You can use the **Exceptions** option to prevent messages from being sent to specific Internet sites.

Prevent Outgoing Messages: Prevent members of the class of service from sending email messages over the Internet. You can use the **Exceptions** option to allow messages to be sent to specific Internet sites.

Prevent Messages Larger Than: This option is available only if you chose **Allow Outgoing Messages** or **Prevent Outgoing Messages**.

If you want to set a size limit on outgoing messages, specify the limit.

Exceptions: This option is available only if you chose **Allow Outgoing Messages** or **Prevent Outgoing Messages**.

If you chose to allow outgoing messages but you want to prevent messages from being sent to specific Internet sites (IP addresses or DNS hostnames), add the sites to the **Prevent Messages To** list.

Conversely, if you chose to prevent outgoing messages but you want to allow messages to be sent to specific Internet sites (IP addresses or DNS hostnames), add the sites to the **Allow Messages To** list.

Allow Replies: This option is available only if you chose **Allow Outgoing Messages** or **Prevent Outgoing Messages**.

This option enables the GWIA to send rule-generated replies to messages (such as vacation rule messages).

In addition, you can use the /blockrulegenmsg startup switch to allow some types of rule-generated messages while blocking others.

Exceptions: Click **Exceptions** to create a list of specific Internet addresses that are handled opposite to the **Allow Replies** setting.

Allow Forwards: This option is available only if you chose **Allow Outgoing Messages** or **Prevent Outgoing Messages**.

This option configures the GWIA to forward rule-generated messages (which can be a security issue).

In addition, you can use the /blockrulegenmsg startup switch to allow some types of rule-generated messages while blocking others.

Exceptions: Click **Exceptions** to create a list of specific Internet addresses that are handled opposite to the **Allow Forwards** setting.

8 Click the **IMAP4** tab, then choose from the following options:

Inherit Access: Members of this class of service inherit their IMAP4 access from a class of service assigned at a higher level. For example, a post office inherits the domain's access. If the domain is not a member of a class of service, the post office inherits the default class of service.

Allow Access: Allow members of the class to send and receive messages with an IMAP4 client.

Prevent Access: Prevent members of the class from sending and receiving messages with an IMAP4 client.

9 Click the **POP3** tab, then choose from the following options:

Inherit Access: Members of this class of service inherit their POP3 access from a class of service assigned at a higher level. For example, a post office inherits the domain's access. If the domain is not a member of a class of service, the post office inherits the default class of service.

Allow Access: Allow members of the class to download their GroupWise messages to a POP3 client.

Prevent Access: Prevent downloading GroupWise messages to a POP3 client.

Delete Messages from GroupWise Mailbox after Download: This option applies only if you selected **Allow Access**.

When you use this option, messages downloaded from a GroupWise Mailbox to a POP3 client are moved to the Trash folder in the GroupWise Mailbox.

POP3 client users can enable this option by using the *user_name*:d login option when initiating their POP session. For more information, see "User Name Login Options" on page 309.

Purge Messages from GroupWise Mailbox after Download: This option applies only if you selected **Allow Access**.

When you use this option, messages downloaded from a GroupWise Mailbox are moved to the Mailbox's Trash folder and then emptied, completely removing the messages from the Mailbox.

POP3 client users can enable this option by using the *user_name*:p login option when initiating their POP session. For more information, see "User Name Login Options" on page 309.

Convert Messages to MIME Format When Downloading: This option applies only if you selected **Allow Access**.

When you use this option, messages downloaded to a POP3 client are converted to the MIME format.

POP3 client users can enable this option by using the *user_name*:m login option when initiating their POP session. They can disable it by using the *user_name*:n login option; this converts messages to RFC-822 format. For more information, see "User Name Login Options" on page 309.

High Performance on File Size Calculations: This option applies only if you selected **Allow Access**.

POP3 clients calculate the size of each message file before downloading it. Enable this option if you want to assign a size of 1 KB to each message file. This eliminates the time associated with calculating a file's actual size.

POP3 client users can enable this option by using the *user_name*:s login option when initiating their POP session. For more information, see "User Name Login Options" on page 309.

Number of Days Prior to Today to Get Messages From: This option applies only if you selected **Allow Access**.

Select the number of days to go back to look for GroupWise Mailbox messages to download to the POP3 client. The default is 30 days.

POP3 client users can override this option by using the *user_name*:t=*x* login option when initiating their POP session. For more information, see "User Name Login Options" on page 309.

Maximum Number of Messages to Download: This option applies only if you selected **Allow Access**.

Select the maximum number of messages a user can download at one time from a GroupWise Mailbox to a POP3 client. The default is 100 messages.

POP3 client users can override this option by using the *user_name*:l=*x* login option when initiating their POP session. For more information, see "User Name Login Options" on page 309.

10 Click **OK** to display the Select GroupWise Object dialog box.

11 Select **Domains**, **Post Offices**, **Groups**, or **Users** to display the list you want.

12 In the list, select the domain, post office, group, or user that you want, then click **OK** to add the object as a member in the class.

    You can Control+click or Shift+click to select multiple objects.

13 To add additional domains, post offices, groups, or users as members of the class of service, select the class of service, then click **Add** to display the Select GroupWise Object dialog box.

14 Click **OK** to add the new class of service to the list.

15 Click **Save**, then click **Close** to return to the main Admin console window.

Managing Classes of Service

1 In the GroupWise Admin console, browse to and click the GWIA.

2 Click the **Access Control** tab, then click **Settings** to display the **Class of Service** list.

3 To edit a class of service, click the name of a class of service.

4 To view the membership of a class of service, highlight the class of service.

5 Click **Save**, then click **Close** to return to the main Admin console window.

Testing Access Control Settings

If you created multiple classes of service, you might not know exactly which settings are being applied to a specific object (domain, post office, group, or user) and which class of service the setting is coming from. To discover an object's settings, you can test the object's access.

1 In the GroupWise Admin console, browse to and click the GWIA.

2 Click the **Access Control** tab, then click **Settings**.

3 Click **Test** to display the Select GroupWise Object dialog box.

4 Select **Domains**, **Post Offices**, **Groups**, or **Users** to display the list you want. For example, if you want to see what access an individual user has, select **Users**.

5 In the list, select the object you want to view, then click **View Access**.

    The tabs show the access control settings for **SMTP Incoming**, **SMTP Outgoing**, **IMAP4**, and **POP3** as they are applied to that user, group, post office, or domain.

6 To view the source for a specific setting, select the setting in the **Setting** box.

7 When you are finished, click **OK**.

Maintaining the Access Control Database

The Access Control database stores the information for the various classes of service you have created. If any problems occur with a class of service, you can validate the database to check for errors with the records and indexes contained in the database. If errors are found, you can recover the database.

The Access database, `gwac.db`, is located in the *domain*\wpgate*gwia* folder.

- "Validating the Database" on page 285
- "Recovering the Database" on page 285

Validating the Database

1. In the GroupWise Admin console, connect to the domain of the GWIA.
2. Browse to and click the GWIA.
3. Click the **Access Control** tab, then click **Database Management**.
4. Click **Validate Now**.
5. After the database has been validated, click **OK**.
6. If errors were found, see Recovering the Database below.

Recovering the Database

If you encountered errors when validating the database, you must recover the database. During the recovery process a new database is created and all intact records are copied to the new database. Some records might not be intact, so you should check the classes of services to see if any information was lost.

1. In the GroupWise Admin console, connect to the domain of the GWIA.
2. Browse to and click the GWIA.
3. Click the **Access Control** tab, then click **Database Management**.
4. Click **Recover Now**.
5. Click **OK**.
6. Check your class of service list to ensure that it is complete.

Blocking Unwanted Email from the Internet

The GWIA includes the following features to help you protect your GroupWise system and users from unwanted email:

- "Real-Time Blacklists" on page 285
- "Access Control Lists" on page 286
- "Blocked.txt File" on page 287
- "Mailbomb (Spam) Protection" on page 287
- "Customized Spam Identification" on page 288
- "SMTP Host Authentication" on page 289
- "Unidentified Host Rejection" on page 290

Real-Time Blacklists

Organizations such as SpamCop (http://www.spamcop.net) provide lists of IP addresses that are known to be open relay hosts or spam hosts. If you want to use free blacklist services such as these, or if you subscribe to fee-based services, you must define the blacklist addresses for these services. The GWIA then uses the defined services to ensure that no messages are received from blacklisted hosts. The following sections provide information to help you define blacklist addresses and, if necessary, override a host address included in a blacklist.

- "Defining a Blacklist Address" on page 286
- "Overriding a Blacklist" on page 286

NOTE: If you want to configure the GWIA to block a specific IP address or DNS hostname, add the address or hostname to a class of service. For more information, see "Controlling User Access to the Internet" on page 279. The Blacklist feature configures the GWIA to use blacklist services that provide real-time lists of many sites that are known to be bad.

Defining a Blacklist Address

1 In the GroupWise Admin console, browse to and click the GWIA.

2 Click the **Access Control** tab, then click **Blacklists**.

The **Blacklist Addresses** list displays the addresses of all blacklists that the GWIA checks when it receives a message from another SMTP host. The GWIA checks the first blacklist and continues checking lists until the sending SMTP host's IP address is found or all lists have been checked. If the sending SMTP host's IP address is included on any of the blacklists, the message is rejected. If you have the GWIA's logging level set to **Verbose**, the log file includes information about the rejected message and the referring blacklist.

This list corresponds with the GWIA's /rbl switch.

3 Click **Add** to display the New Blacklist Address dialog box.

For example, for SpamCop (http://www.spamcop.net), you would use the following address:

```
bl.spamcop.net
```

4 Type the blacklist address in the **Address** box, then click **OK** to add the address to the **Blacklist Addresses** list.

5 If you have multiple blacklists in the **Blacklist Addresses** list, use the up-arrow and down-arrow to position the blacklists in the order you want them checked. The GWIA checks the blacklists in the order they are listed, from top to bottom.

6 Click **Save**, then click **Close** to return to the main Admin console window.

Overriding a Blacklist

In some cases, a blacklist might contain a host from which you still want to receive messages. For example, goodhost.com has been accidentally added to a blacklist but you still want to receive messages from that host.

You can use the **SMTP Incoming Exceptions** list on a class of service to override a blacklist. For information about editing or creating a class of service, see "Creating a Class of Service" on page 281.

Access Control Lists

If you want to block specific hosts yourself rather than use a blacklist (in other words, create your own blacklist), you can configure a class of service that prevents messages from those hosts. You do this on the GWIA object's **Access Control Settings** tab by editing the desired class of service to add the hosts to the **Prevent Messages From** exception list on the **SMTP Incoming** tab. For example, if you wanted to block all messages from badhost.com, you could edit the default class of service to add badhost.com to the list of prevented hosts.

You can also create a list of hosts that you always want to allow messages from, so you can create your own white list.

For information about editing or creating a class of service, see "Creating a Class of Service" on page 281.

Blocked.txt File

The GroupWise Admin console creates a `blocked.txt` file in the `domain/wpgate/gwia` folder that includes all the hosts that have been added to the **Prevent Messages From** exceptions list for the default class of service (see “Controlling User Access to the Internet” on page 279).

You can manually edit the `blocked.txt` file to add or remove hosts. To maintain consistency for your system, you can also copy the list to other GWIA installations.

To manually edit the `blocked.txt` file:

1. Open the `blocked.txt` file in a text editor.
2. Add the host addresses.

   The entry format is:

   `address1 address2 address3`

   where *address* is either a hostname or an IP address. You can block on any octet. For example:

IP Address	Blocks
..*.34	Any IP address ending with 34
172.16.*.34	Any IP address starting with 172.16 and ending with 34
172.16.10-34.*	Any IP address starting with 172.16 and any octet from 10 to 34

   You can block on any segment of the hostname. For example:

Hostname	Blocks
provo*.novell.com	provo.novell.com provo1.novell.com provo2.novell.com
*.novell.com	gw.novell.com (but not novell.com itself)

   There is no limit to the number of IP addresses and hostnames that you can block in the `blocked.txt` file
3. Save the file as `blocked.txt`.

Mailbomb (Spam) Protection

Multiple unsolicited messages (sometimes called a *mailbomb* or *spam*) from the Internet can potentially harm your GroupWise messaging environment. You can use the settings on the SMTP/MIME **Security Settings** tab to help protect your GroupWise system from malicious or accidental attacks.

To configure the SMTP security settings:

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **SMTP/MIME** tab, then click **Security Settings**.
3. Fill in the fields:

   Reject if PTR Record Does Not Exist: This setting lets you prevent messages if the sender’s host is not authentic.

When this setting is turned on, the GWIA refuses messages from a smart host if a DNS reverse lookup shows that a PTR record does not exist for the IP address of the sender's host.

When this setting is turned off, the GWIA accepts messages from any host, but displays a warning if the initiating host is not authentic.

This setting corresponds with the GWIA's /rejbs switch.

- **Reject If PTR Record Does Not Match Sender's Greeting:** Configure the GWIA to reject messages from sending SMTP hosts where the sending host's PTR record does not match the information that the SMTP host sends out when it is initially contacted by another SMTP host. If the information does not match, the sending host might not be authentic.
- **Flag Messages with an Invalid PTR Record as Junk Mail:** Allow messages from unidentified sources to be handled by users' Junk Mail Handling settings in the GroupWise client rather than by being rejected by the GWIA. This gives users more control over what they consider to be junk mail.

Enable Mailbomb Protection: Mailbomb protection is turned off by default. You can turn it on by selecting this option.

Mailbomb Threshold: When you enable Mailbomb protection, default values are defined in the threshold settings. The default settings are 30 messages received within 10 seconds. You can change the settings to establish an acceptable security level.

Any group of messages that exceeds the specified threshold settings is entirely discarded. If you want to prevent future mailbombs from the mailbomb sender, identify the sender's IP address (by looking at the GWIA's console) and then modify the appropriate class of service to prevent mail being received from that IP address (**Access Control > Settings**). For more information, see "Creating a Class of Service" on page 281.

The time setting corresponds with the GWIA's /mbtime switch. The message count setting corresponds with the /mbcount switch.

4. Click **Save**, then click **Close** to return to the main Admin console window.

For additional protective startup switches, see "Mailbomb and Spam Security" on page 344.

Customized Spam Identification

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **SMTP/MIME** tab, then click **Junk Mail**.
3. Select **Flag Any Messages**, then specify the strings in the text box.

   Anti-spam services use different indicators to mark potential spam. One might use a string of asterisks; the more asterisks, the greater the likelihood that the message is spam. Another might use a numerical value; the higher the number, the greater the likelihood that the message is spam. The following samples are taken from MIME headers of messages:

   `X-Spam-Results: ***** X-Spam-Status: score=9`

   Based on these samples, examples are provided below of lines that you could add to the list to handle the X-Spam tags found in the MIME headers of messages coming into your system.

   Example: `X-Spam-Results: *****`

   This line marks as spam any message whose MIME header contained an X-Spam-Results tag with five or more asterisks. Messages with X-Spam-Results tags with fewer than five asterisks are not marked as spam.

   Example: `X-Spam-Status: Yes`

   This line marks as spam any message whose MIME header contained the X-Spam-Status tag set to Yes, regardless of the score.

Example: `X-Spam-Status: score=9` `X-Spam-Status: score=10`

These lines marks as spam any message whose MIME header has the X-Spam-Status tag set to Yes and had a score of 9 or 10. X-Spam-Status tags with scores less than 9 are not marked as spam.

You can add as many lines as necessary to the list to handle whatever message tagging your anti-spam service uses.

4 Click **Save**, then click **Close** to return to the main Admin console window.

The list is saved in the `xspam.cfg` file in the *domain*\wpgate*gwia* folder. As described above, each line of the `xspam.cfg` file identifies an "X" header field that your anti-spam service is writing to the MIME header, along with the values that flag the message as spam. The GWIA examines the MIME header for any field listed in the `xspam.cfg` file. When a match occurs, the message is marked for handling by the GroupWise client Junk Mail Handling feature.

SMTP Host Authentication

The GWIA supports SMTP host authentication for both outbound and inbound message traffic.

- "Outbound Authentication" on page 289
- "Inbound Authentication" on page 289

Outbound Authentication

For outbound authentication to other SMTP hosts, the GWIA requires that the remote SMTP hosts support the AUTH LOGIN authentication method. To set up outbound authentication:

1 Include the remote SMTP host's domain name an authentication credentials in the `gwauth.cfg` file, located in the *domain*\wpgate*gwia* folder. The format is:

```
domain_name   authuser   authpassword
```

For example:

```
smtp.novell.com   remotehost   novell
```

2 If you have multiple SMTP hosts that require authentication before they accept messages from your system, create an entry for each host. Ensure include a hard return after the last entry.

3 If you want to allow the GWIA to send messages only to SMTP hosts listed in the `gwauth.cfg` file, use the following startup switch:

```
/forceoutboundauth
```

With the --forceoutboundauth switch enabled, if a message is sent to an SMTP host not listed in the `gwauth.cfg` file, the sender receives an Undeliverable message.

Inbound Authentication

For inbound authentication from other SMTP hosts, you can use the --forceinboundauth startup switch to ensure that the GWIA accepts messages only from SMTP hosts that use the AUTH LOGIN authentication method to provide a valid GroupWise use name and password. The remote SMTP hosts can use any valid GroupWise user name and password. However, for security reasons, we recommend that you create a dedicated GroupWise user account for remote SMTP host authentication.

Unidentified Host Rejection

You can use the --rejbs switch to have the GWIA reject messages from unidentified sources. The GWIA refuses messages from a host if a DNS reverse lookup shows that a “PTR” record does not exist for the IP address of the sender’s host.

By default, the GWIA does not reject messages from unidentified hosts. It accepts messages from any host, but it displays a warning if the sender’s host is not authentic.

Tracking Internet Traffic with Accounting Data

The GWIA can supply accounting information for all messages, including information such as the message’s source, priority, size, and destination.

The accounting file is an ASCII-delimited text file that records the source, priority, message type, destination, and other information about each message sent through the gateway. The file, which is updated daily at midnight (and each time the GWIA restarts), is called `acct` and is located in the *xxx*`.prc` folder. If no accountant is specified for the gateway in the GroupWise Admin console, the file is deleted and re-created each day. Follow the steps below to set up accounting.

- “Selecting an Accountant” on page 290
- “Enabling Accounting” on page 290
- “Understanding the Accounting File” on page 290
- “Generating an Accounting Report” on page 292

Selecting an Accountant

You can select one or more GroupWise users to be accountants. Every day at midnight, each accountant receives an accounting file (`acct`) that contains information about the messages the gateway sent that day.

1. In the GroupWise Admin console, browse to and click the GWIA.
2. On the **GroupWise** tab, click **Administrators**.
3. Click **Add**, browse for and select the user you want to add, then click **OK** to add the user to the list of administrators.
4. Select the user in the list of administrators, then click **Accountant**.
5. Click **Save**, then click **Close** to return to the main Admin console window.

Enabling Accounting

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **GroupWise** tab, then click **Optional Settings**.
3. Set **Accounting** to **Yes**.
4. Set **Correlation Enabled** to **Yes**.
5. Click **Save**, then click **Close** to return to the main Admin console window.

Understanding the Accounting File

The following is an Accounting file entry for a single event. Each field in the entry is described below.

```
O,1/25/18,21:58:39,3DE29CD2.14E:7:6953, Mail,2,Provo,Research,jsmith,48909,Meeting
Agenda,Provo,GWIA,sde23a9f.001,MIME,hjones@novell.com,1,2,11388,0
```

Field	Example	Description
Inbound/Outbound	`O`	Displays `I` for inbound messages and `O` for outbound messages
Date	`1/25/18`	The date the message was processed.
Time	`21:58:39`	The time the message was processed.
GroupWise message ID	`3DE29CD2.14E:7:6953`	The unique GroupWise ID assigned to the message.
GroupWise message type	`Mail`	Mail message, appointment, task, note, or phone message for outbound messages. Unknown for inbound messages.
GroupWise message priority	`2`	High priority = 1 Normal priority = 2 Low priority = 3
GroupWise user's domain	`Provo`	The domain in which the GroupWise user resides.
GroupWise user's post office	`Research`	The post office where the GroupWise user's mailbox resides.
GroupWise user's ID	`jsmith`	The GroupWise user name. For outbound messages, the GroupWise user is the message sender. For inbound messages, the GroupWise user is the message recipient.
GroupWise user's account ID	`48909`	The GroupWise user name.
Message subject	`Meeting Agenda`	The message's Subject line. Only the first 32 characters are displayed.
Gateway domain	`Provo`	The domain where the GWIA resides.
Gateway name	`GWIA`	The GWIA's name.
Foreign message ID	`sde23a9f.001`	A unique ID for outbound messages. The identifier before the period (sde23a9f) uniquely identifies a message. The identifier after the period (001) is incremented by one for each message sent.
Foreign message type	`MIME`	The message type (MIME, etc.)
Foreign user's address	`hjones@novell.com`	The foreign user's email address. For inbound messages, the foreign user is the message sender. For outbound messages, the foreign user is the message recipient.
Recipient count	`1`	The number of recipients.
Attachment count	`2`	The number of attached files. The total count includes the message.
Message size	`11388`	The total size, in bytes, of the message and its attachments.
Other	`0`	Not used.

Generating an Accounting Report

You can use the Monitor Agent to generate a report based on the contents of this file. For more information, see "Gateway Accounting Report" on page 664.

30 Configuring SMTP/MIME Services

SMTP and MIME are standard protocols that the GWIA uses to send and receive email messages over the Internet. SMTP, or Simple Mail Transfer Protocol, is the message transmission protocol. MIME, or Multipurpose Internet Mail Extension, is the message format protocol. Choose from the following topics for information about how to enable SMTP/MIME services and configure various SMTP/MIME settings:

Configuring Basic SMTP/MIME Settings

Basic SMTP/MIME settings configure the following aspects of GWIA functioning:

- Number of send and receive threads that the GWIA starts and how often the send threads poll for outgoing messages
- Hostname of the server where the GWIA is running and of a relay host if your system includes one
- IP address to bind to at connection time if the server has multiple IP addresses
- Whether to use 7-bit or 8-bit encoding for outgoing messages
- How to handle messages that cannot be sent immediately and must be deferred
- Whether to notify senders when messages are delayed
- Whether to display GroupWise version information when establishing an SNMP connection

To set the GWIA basic SMTP/MIME settings:

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **SMTP/MIME** tab, then click **Settings**.
3. Fill in the fields:

   Enable SMTP Service: SMTP service is on by default. This setting corresponds with the GWIA's --smtp switch.

   Number of SMTP Send Threads: The SMTP send threads setting lets you specify the number of threads that process SMTP send requests. Each thread is equivalent to one connection. The default is 8 threads. This setting corresponds with the GWIA's --sd switch.

   Number of SMTP Receive Threads: The SMTP receive threads setting lets you specify the number of threads that process SMTP receive requests. Each thread is equivalent to one connection. The default is 16 threads. This setting corresponds with the GWIA's --rd switch.

   Kill Threads on Exit or Restart: Configure the GWIA to stop immediately, without allowing its send/receive threads to perform their normal shutdown procedures. The normal termination of all send/receive threads can take several minutes, especially if a large message is being processed. By terminating immediately, a needed restart can occur immediately as well. This setting corresponds with the GWIA's --killthreads switch.

   Enable iCal Service: Configure the GWIA to convert outbound GroupWise Calendar items into MIME text/calendar iCal objects and to convert incoming MIME text/calendar messages into GroupWise Calendar items. Enabling the iCal service provides the functionality described in "Accepting or Declining Internet Items" in the *GroupWise 18 Client User Guide*. This setting corresponds with the GWIA's --imip switch.

Hostname/DNS "A Record" Name: The Hostname/DNS "A Record" name setting lets you identify the hostname of the server where the GWIA resides, or in other words the A Record in your DNS table that associates a hostname with the server's IP address (for example, `gwia.novell.com`). This setting corresponds with the GWIA's --hn switch.

If you leave this field blank, the GWIA uses the hostname obtained by querying the hosts file from the server.

Relay Host for Outbound Messages: The relay host setting can be used if you want to use one or more relay hosts to route all outbound Internet email. Specify the IP address or DNS hostname of the relay hosts. Use a space between relay hosts in a list. Relay hosts can be part of your network or can reside at the Internet service provider's site. This setting corresponds with the GWIA's --mh switch.

If multiple hosts are specified, they are used in a round robin fashion with the GWIA starting over at the top of the list each time the GWIA is started. If there is an error sending through one host, the error will be logged in the GWIA logs and the GWIA will use the next host in the list. As long as the error wasn't a fatal error, the message that failed to send will be placed in a deferred folder and the GWIA will follow the intervals configured for deferred messages. If a fatal error is received, the GWIA will stop attempting to contact the host and report the error message in the GWIA logs.

If you want to use a relay host, but you want some outbound messages sent directly to the destination host rather than to the relay host, you can use a route configuration file (`route.cfg`). Whenever a message is addressed to a user at a host that is included in the `route.cfg` file, the GWIA sends the message directly to the host rather than to the relay host. For information about creating a `route.cfg` file, see "Using a Route Configuration File" on page 301.

Scan Cycle for Send Directory: The Scan cycle setting specifies how often the GWIA polls for outgoing messages. The default is 10 seconds. This setting corresponds with the GWIA's --p switch.

Use 7 Bit Encoding for All Outbound Messages: By default, the GWIA uses 8-bit MIME encoding for any outbound messages that are HTML-formatted or that contain 8-bit characters. If, after connecting with the receiving SMTP host, the GWIA discovers that the receiving SMTP host cannot handle 8-bit MIME encoded messages, the GWIA converts the messages to 7-bit encoding.

With this option selected, the GWIA automatically uses 7-bit encoding and does not attempt to use 8-bit MIME encoding. You should use this option if you are using a relay host that does not support 8-bit MIME encoding. This setting corresponds with the GWIA's --force7bitout switch.

Maximum Number of Hours to Retry a Deferred Message: Specify the number of hours after which the GWIA stops trying to send deferred messages. The default is 96 hours (4 days). You might prefer to receive an undeliverable notification sooner, perhaps in as little as 5 hours. A deferred message is any message that can't be sent because of a temporary problem (host down, MX record not found, and so on). This setting corresponds with the GWIA's --maxdeferhours switch.

Intervals to Retry a Deferred Message: Specify in a comma-delimited list the number of minutes after which the GWIA retries sending deferred messages. The default is 20, 20, 20, 60. The GWIA interprets this list as follows: It retries 20 minutes after the initial send, 20 minutes after the first retry, 20 minutes after the second retry, and 60 minutes after the third retry. Thereafter, it retries based on the final retry interval until the number of hours specified in the **Maximum Number of Hours to Retry a Deferred Message** field is reached. You can provide additional retry intervals as needed. It is the last retry interval that repeats until the maximum number of hours is reached. This setting corresponds with the GWIA's --msgdeferinterval switch.

Return Notification to Sender When a Message Is Delayed: Provide a notification message to users whose email messages cannot be immediately sent out across the Internet. This provides more noticeable notification to users than manually checking the Properties page of the sent item to see whether it has been sent. This setting corresponds with the GWIA's --delayedmsgnotification switch.

Do Not Publish GroupWise Information on an Initial SMTP Connection: This option suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by another SMTP host or a telnet session. It is enabled by default. This setting corresponds with the GWIA's --nosmtpversion switch.

4. Click **Save**, then click **Close** to return to the main Admin console window.

Using Extended SMTP (ESMTP) Options

The GWIA supports several Extended SMTP (ESMTP) settings. These are settings that might or might not be supported by another SMTP system.

The following ESMTP extensions are supported:

- **SIZE:** For more information, see RFC 1870 (http://www.ietf.org/rfc/rfc1870.txt).
- **AUTH:** For more information, see RFC 2554 (http://www.ietf.org/rfc/rfc2554.txt).
- **DSN:** For more information, see RFC 3464 (http://www.ietf.org/rfc/rfc3464.txt) and RFC 3461 (http://www.ietf.org/rfc/rfc3461.txt).
- **8BITMIME:** For more information, see RFC 1652 (http://www.ietf.org/rfc/rfc1652.txt).
- **STARTTLS:** For more information, see RFC 3207 (http://www.ietf.org/rfc/rfc3207.txt).

To configure ESMTP settings:

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **SMTP/MIME** tab, then click **ESMTP**.
3. Choose from the following options:
   - **Enable Delivery Status Notification:** Configure the GWIA to request status notifications for outgoing messages and to supply status notifications for incoming messages. This requires the external email system to also support **Delivery Status Notification**. Currently, notification consists of two delivery statuses: successful or unsuccessful.

     If you enable the **Delivery Status Notification** option, you need to select the number of days that you want the GWIA to retain information about the external sender so that status updates can be delivered to him or her. For example, the default hold age causes the sender information to be retained for 4 days. If the GWIA does not receive delivery status notification from the GroupWise recipient's Post Office Agent (POA) within that time period, it deletes the sender information and the sender does not receive any delivery status notification.

     If you enable this option for the GWIA, it overrides what GroupWise client users set under **Tools > Options > Send > Mail > Send Notification to My Mailbox**. By default, this option is deselected in the GroupWise client, but if you select **Enable Delivery Status Notification** in the GroupWise Admin console, users receive delivery status notifications in their mailboxes even when the option is deselected in the GroupWise client.
   - **Require SSL for authentication:** When enabled, this option requires an SMTP sender to negotiate a secure connection before GWIA would advertise that AUTH is supported.

* **Force inbound authentication:** Ensures that the Internet Agent accepts messages only from remote SMTP hosts that use the AUTH LOGIN authentication method to provide a valid GroupWise user ID and password.
* **Force outbound authentication:** Ensures that the Internet Agent sends messages only to remote SMTP hosts that are included in a `gwauth.cfg` file.
* **Disable ESMTP extensions:** Disables all ESMTP extensions in the Internet Agent. Generally used only for troubleshooting purposes.

4 Click **Save**, then click **Close** to return to the main Admin console window.

Configuring How the GWIA Handles Email Addresses

The GWIA can handle email addresses in a variety of ways:

* Internet addressing vs. GroupWise proprietary addressing
* Group membership expansion on inbound messages
* Distribution membership expansion on outbound messages
* Using non-GroupWise domains
* Using sender's address format
* Using domain and post office information

To set the GWIA address handling options:

1 In the GroupWise Admin console, browse to and click the GWIA.

2 Click the **SMTP/MIME** tab, then click **Address Handling**.

3 Fill in the fields:

Ignore GroupWise Internet Addressing: GroupWise supports both Internet-style addressing (*user@host*) and GroupWise proprietary addressing (*user_name*.*post_office*.*domain*). By default, the GWIA uses Internet-style addressing.

The GWIA supports user and post office aliases in either mode. This setting corresponds with the GWIA's --dia switch.

Expand Groups on Incoming Messages: When incoming Internet messages are addressed to a group, send the message to all members of the group. This setting corresponds with the GWIA's --group switch. See also the --nickgroup switch to enable group expansion for groups that have nicknames.

Do Not Replace Underscores with Spaces: Configure the GWIA to convert not user names in email addresses from the format Firstname_Lastname into the format Firstname Lastname by replacing the underscore with a space. By default, this conversion takes place automatically, even though Firstname_Lastname is not an address format that is included in the **Allowed Address Formats** list in the Internet Addressing dialog box. This setting corresponds with the GWIA's --dontreplaceunderscore switch.

Non-GroupWise Domain for RFC-822 Replies: This setting can be used only if 1) you created a non-GroupWise domain to represent all or part of the Internet, and 2) you defined the non-GroupWise domain's outgoing conversion format as RFC-822 when you linked the GWIA to the domain. For more information, see "Adding External Users to the GroupWise Address Book" on page 78.

Specify the name of the non-GroupWise domain associated with the RFC-822 conversion format. When a GroupWise user replies to a message that was originally received by the GWIA in RFC-822 format, the reply is sent to the specified non-GroupWise domain and converted to RFC-822 format so that it is in the same format as the original message.

This setting corresponds with the GWIA's --fd822 switch.

Non-GroupWise Domain for MIME Replies: This setting can be used only if 1) you created a non-GroupWise domain that represents all or part of the Internet, and 2) you defined the non-GroupWise domain's outgoing conversion format as MIME when you linked the GWIA to the domain. For more information, see "Adding External Users to the GroupWise Address Book" on page 78.

Specify the name of the non-GroupWise domain associated with the MIME conversion format. When a GroupWise user replies to a message that was originally received by the GWIA in MIME format, the reply is sent to the specified non-GroupWise domain and converted to MIME format so that it is in the same format as the original message.

This setting corresponds with the GWIA's --fdmime switch.

Sender's Address Format: This setting applies only if you have not enabled GroupWise Internet addressing (in other words, you selected the **Ignore GroupWise Internet Addressing** option). If GroupWise Internet addressing is enabled, the GWIA ignores this setting and uses the preferred address format established for outbound messages (**Tools > GroupWise System Operations > Internet Addressing**).

The Sender's Address Format setting lets you specify which GroupWise address components (*domain*.*post_office*.*user_name*) are included as the user portion of the address on outbound messages. You can choose from the following options:

- **Domain, Post Office, User, and Hostname:** Uses the *domain*.*post_office*.*user_name*@*host* syntax.
- **Post Office, User, and Hostname:** Uses the *post_office*.*user_name*@*host* syntax.
- **User and Hostname:** Uses the *user_name*@*host* syntax.
- **Auto (default):** Uses the GroupWise addressing components required to make the address unique within the user's GroupWise system. If a user name is unique in a GroupWise system, the outbound address uses only the user name. If the post office or domain.post office components are required to make the address unique, these components are also included in the outbound address.

The Sender's Address Format setting corresponds with the GWIA's --aql switch.

Place Domain and Post Office Qualifiers: If the sender's address format must include the domain and/or post office portions to be unique, you can use this option to determine where the domain and post office portions are located within the address.

- **On Left of Address (default):** Leaves the domain and post office portions on the left side of the @ sign (for example, *domain*.*post_office*.*user_name*@*host*.
- **On Right of Address:** Moves the domain and post office portions to the right side of the @ sign, making the domain and post office part of the host portion of the address (for example, *user_name*@*post_office*.*domain*.*host*. If you choose this option, you must ensure that your DNS server can resolve each *post_office*.*domain*.*host* portion of the address. This setting corresponds with the GWIA's --aqor switch.

  Retain Groups on Outgoing Messages: When constructing the MIME for outgoing messages, discard all users that expanded out of system distribution lists. Instead include a reference to the distribution list. This results in a smaller MIME and Reply to All list for the recipient. This setting corresponds with the GWIA's --keepsendgroups switch.

  NOTE: If you retain groups on outgoing messages, Reply to All might not work unless you also enable inbound group expansion by using the --group switch.

Use GroupWise User Address as Mail From: for Rule Generated Messages: Configure the GWIA to use the real user in the **Mail From** field instead of having auto-forwards come from Postmaster and auto-replies come from Mailer-Daemon. This setting corresponds with the GWIA's --realmailfrom switch.

4 Click **Save**, then click **Close** to return to the main Admin console window.

Determining Format Options for Messages

You can control aspects of how the GWIA formats incoming and outgoing messages:

- Number of GWIA threads for converting messages into the specified format
- The view in which incoming messages are displayed to GroupWise users
- Text encoding method (Basic RFC-822 or MIME)
- Text wrapping
- Message prioritization based on x-priority fields

To set the GWIA format options:

1 In the GroupWise Admin console, browse to and click the GWIA.

2 Click the **SMTP/MIME** tab, then click **Message Formatting**.

3 Fill in the fields:

Number of Inbound Conversion Threads: The inbound conversion threads setting lets you specify the number of threads that convert inbound messages from MIME or RFC-822 format to the GroupWise message format. The default setting is 4. This setting corresponds with the GWIA's --rt switch.

Number of Outbound Conversion Threads: The outbound conversion threads setting lets you specify the number of threads that convert outbound messages from the GroupWise message format to MIME or RFC-822 format. The default setting is 4. This setting corresponds with the GWIA's --st switch.

Default Message Encoding: The default message encoding setting lets you select the encoding method for your outbound Internet messages. You can select either **Basic RFC-822** formatting or **MIME** formatting. **MIME** is the default message format. This setting corresponds with the GWIA's --mime switch.

If you select the **Basic RFC-822** option, you can decide whether or not to have the GWIA UUEncode all ASCII text attachments to RFC-822 formatted messages. By default, this option is turned off, which means ASCII text attachments are included as part of the message body. This setting corresponds with the GWIA's --uueaa switch.

NOTE: RFC-822 is a very old format. Use it only if you have a specific need for it.

Message Text Line Wrapping: The **Quoted Printable** text line wrapping setting lets you select the Quoted Printable MIME standard for line wrapping, which provides "soft returns". By default this setting is turned on. If you turn the setting off, MIME messages go out as plain text and wrap text with "hard returns" according to the number of characters specified in the line wrap length setting. This setting corresponds with the GWIA's --nqpmt switch.

The **Line Wrap Length for Message Text on Outbound Mail** setting lets you specify the line length for outgoing messages. This is useful if the recipient's email system requires a certain line length. The default line length is 72 characters. This setting corresponds with the GWIA's --wrap switch.

Enable Flat Forwarding: Automatically strip out the empty message that is created when a message is forwarded without adding text, and retain the original sender of the message, rather than showing the user who forwarded it. This facilitates users forwarding messages from GroupWise to other email accounts. Messages arrive in the other accounts showing the original senders, not the users who forwarded the messages from GroupWise. This setting corresponds with the GWIA's --flatfwd switch.

Default Global Signature to Insert in Outbound Messages: Displays the default global signature for your GroupWise system. If you want this GWIA to append a different global signature, select **Override**, then select the desired signature. For more information, see "Setting a Default Global Signature" on page 460.

Apply Global Signature to Relay Messages: Append the global signature to messages that are relayed through your GroupWise system (for example, messages from POP and IMAP clients) in addition to messages that originate within your GroupWise system. This setting corresponds with the GWIA's --relayaddsignature switch.

Disable Mapping X-Priority Fields: Disable the function of mapping an x-priority MIME field to a GroupWise priority for the message. By default, the GWIA maps x-priority 1 and 2 messages as high priority, x-priority 3 messages as normal priority, and x-priority 4 and 5 as low priority in GroupWise. This setting corresponds with the GWIA's --nomappriority switch.

4. Click **Save**, then click **Close** to return to the main Admin console window.

Configuring the SMTP Timeout Settings

The SMTP Timeout settings specify how long the GWIA's SMTP service waits to receive data that it can process. After the allocated time expires, the GWIA might give a TCP read/write error.

To configure the SMTP timeout settings:

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **SMTP/MIME** tab, then click **Timeouts**.
3. Fill in the fields:

   Commands: The **Commands** setting lets you specify how long the GWIA waits for an SMTP command. The default is 5 minutes. This setting corresponds with the GWIA's --tc switch.

   Data: The **Data** setting lets you specify how long the GWIA waits for data from the receiving host. The default is 3 minutes. This setting corresponds with the GWIA's --td switch.

   Connection Establishment: The **Connection Establishment** setting lets you specify how long the GWIA waits for the receiving host to establish a connection. The default is 2 minutes. This setting corresponds with the GWIA's --te switch.

   Initial Greeting: The **Initial Greeting** setting lets you specify how long the GWIA waits for the initial greeting from the receiving host. The default is 5 minutes. This setting corresponds with the GWIA's --tg switch.

   TCP Read: The **TCP Read** setting lets you specify how long the GWIA waits for a TCP read. The default is 5 minutes. This setting corresponds with the GWIA's --tr switch.

   Connection Termination: The **Connection Termination** setting lets you specify how long the GWIA waits for the receiving host to terminate the connection. The default is 10 minutes. This setting corresponds with the GWIA's --tt switch.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Determining What to Do with Undeliverable Messages

You can configure how the GWIA handles messages that it cannot deliver:

- How much of the message to return to the sender
- Another host to forward the message to (where it might be deliverable)
- Whether to move the message to the GroupWise problem folder or send it to the GroupWise administrator

To set the GWIA undeliverable message options:

1 In the GroupWise Admin console, browse to and click the GWIA.

2 Click the **SMTP/MIME** tab, then click **Undeliverables**.

3 Fill in the fields:

   Amount of Original Message to Return to Sender When Message is Undeliverable: This setting lets you specify how much of the original message is sent back to the sender when a message is undeliverable. By default, only 2 KB of the original message is sent back. This setting corresponds with the GWIA's --mudas switch.

   Forward Undeliverable Inbound Messages to Host: This setting lets you specify a host to which undeliverable messages are forwarded.

   When an IP address is specified rather than a DNS hostname, the IP address must be surrounded by square brackets [ ]. For example, [172.16.5.18].

   This setting corresponds with the GWIA's --fut switch.

   Problem Messages: These settings allow you specify what you want the GWIA to do with problem messages. A problem message is an inbound or outbound message that the GWIA cannot convert properly. By default, problem messages are discarded. If you want to save problem messages, specify whether to move the messages to the problem directory (`gwprob`), send them to the postmaster, or do both. This setting corresponds with the GWIA's --badmsg switch.

4 Click **Save**, then click **Close** to return to the main Admin console window.

Enabling SMTP Relaying

You can enable the GWIA to function as a relay host for Internet messages. The GWIA can relay messages received from all Internet hosts, or you can select specific hosts for which you allow it to relay.

1 In the GroupWise Admin console, browse to and click the GWIA.

2 Click the **Access Control** tab, then click **SMTP Relay Settings**.

3 Under **SMTP Relay Defaults**, select whether you want to allow or prevent message relaying.

   If you prevent message relaying, you can define exceptions that allow message relaying for specific Internet hosts. This can also be done if you allow message relaying. We suggest that you select the option that enables you to define the fewest exceptions.

4 To prevent relaying of messages larger than a specific size (regardless of the **SMTP Relay Defaults** setting), enable the **Prevent Messages Larger Than** option and specify the size limitation.

5 To define an exception, click **New** to display the New Internet Address dialog box.

6 Fill in the following fields:

From: Specify the Internet address that must be in the message's **From** field for the exception to be applied.

To: Specify the Internet address that must be in the message's **To** field for the exception to be applied. This is also the address that the message is relayed to (in the case of an Allow exception).

In both the **From** and **To** fields, you can use either an IP address or a DNS hostname, as shown in the following examples:

```
novell.com
10.1.1.10
```

You can enter a specific address, as shown above, or you can use wildcards and IP address ranges to specify multiple addresses, as follows:

```
*.novell.com
10.1.1.*
10.1.1.10-15
```

NOTE: If the user for whom you want to define an exception has an alias, you must also define an exception for the user's alias. Ongoing use of aliases is not recommended.

---

7 Click **OK** to add the exception to the list.

8 Click **Save**, then click **Close** to return to the main Admin console window.

Using a Route Configuration File

The GWIA supports the use of a route configuration file (`route.cfg`) to specify destination SMTP hosts. This can be useful in situations such as the following:

- You are using a relay host for outbound messages. However, you want some outbound messages sent directly to the destination host rather than the relay host. Whenever a message is addressed to a user at a host that is included in the `route.cfg` file, the GWIA sends the message directly to the destination host rather than the relay host.
- You need to send messages to SMTP hosts that are unknown to the public Domain Name Servers. The `route.cfg` file acts much like a hosts file to enable the GWIA to resolve addresses not listed in DNS.
- The GWIA uses external DNS servers but the server it is running on has an internal IP address. This prevents the GWIA from querying external DNS servers for its own internal domain names and receiving Host Down errors from the external DNS servers.
- You want to route messages through an SMTP host that checks for viruses (or performs some other task) before routing them to the destination host.

To set up a `route.cfg` file:

1 Create the `route.cfg` file as a text file in the *`domain`*`\wpgate\`*`gwia`* folder.

2 Add an entry for each SMTP host you want to send to directly. The entry format is:

```
hostname  address
```

Replace *`hostname`* with a DNS hostname or an Internet domain name. Replace *`address`* with an alternative hostname or an IP address. For example:

```
novell.com gwia.novell.com
unixbox [172.16.5.18]
```

If you use an IP address, it must be included in square brackets, as shown above.

To reference subdomains, place a period (.) in front of the domain name as a wildcard character. For example:

```
.novell.com gwia.novell.com
```

Ensure that you include a hard return after the last entry.

3 Save the `route.cfg` file.

4 Restart the GWIA.

Customizing Delivery Status Notifications

The GWIA returns status messages for all outbound messages. For example, if a GroupWise user sends a message that the GWIA cannot deliver, the GWIA returns an undeliverable message to the GroupWise user.

By default, the GWIA uses internal status messages. However, you can override the internal status messages by using a `status.xml` file that includes the status messages you want to use.

1 Open the appropriate `status`*`xx`*`.xml` file, located in the *`domain`*`\wpgate\`*`gwia`* folder.

   The *`domain`*`\wpgate\`*`gwia`* folder includes a `status`*`xx`*`.xml` file for each language included in the downloaded *GroupWise 18* software image (for example, `statusus.xml`, `statusde.xml`, and `statusfr.xml`).

2 Make the modifications you want.

   The following sample code shows the elements and default text of the Undeliverable Message status:

```
<STATUS_MESSAGE type="undeliverableMessage" xml:lang="en-US">
<SUBJECT>Message status - undeliverable</SUBJECT>
<MESSAGE_BODY>
<TEXT>\r\nThe attached file had the following undeliverable recipient(s):\r\n</
TEXT>
<RECIPIENT_LIST format="\t%s\r\n"
<SESSION_TRANSCRIPT>
<TEXT>\r\nTranscript of session follows:\r\n<TEXT>
</SESSION_TRANSCRIPT>
<ATTACH_ORIGINAL_MSG></ATTACH_ORIGINAL_MSG>
</MESSAGE_BODY>
</STATUS_MESSAGE>
```

   You can modify text in the `<SUBJECT>` tag or in the `<TEXT>` tags.

   You can add additional `<TEXT> tags` in the `<MESSAGE_BODY>`.

   You can remove tags to keep an element from being displayed. For example, you could remove the `<ATTACH_ORIGINAL_MSG></ATTACH_ORIGINAL_MSG>` tags to keep the original message from displaying.

   You can use the following format characters and variables:

   - \t: tab
   - \r: carriage return
   - \n: line feed
   - %s: recipient name variable

3 Save the file, renaming it from `statusxx.xml` to `status.xml`.

4 Restart the GWIA.

The GWIA now uses the status messages defined in the `status.xml` file rather than its internal status messages.

Managing MIME Messages

Multipurpose Internet Mail Extensions, or MIME, provides a means to interchange text in languages with different character sets. Multimedia email can be sent between different computer systems that use the SMTP protocol. MIME enables you to send and receive email messages containing:

- Images
- Sounds
- Linux Tar Files
- PostScript
- FTP-able File Pointers
- Non-ASCII Character Sets
- Enriched Text
- Nearly any other file

Because MIME handles such a variety of file types, you might need to customize aspects of MIME for your users.

- "Customizing MIME Preamble Text" on page 303
- "Customizing MIME Content-Type Mappings" on page 304

Customizing MIME Preamble Text

An ASCII file called `preamble.txt` is installed in the GWIA gateway folder (*domain*`\wpgate\`*gwia*). This file, which is included with any MIME multipart message, is displayed when the message recipient lacks a MIME-compliant mail reader.

The content of the `preamble.txt` file is a warning, in English, that the file is being sent in MIME format. If the recipient cannot read the message, he or she needs to either use a MIME-compliant mail reader or reply to the sender and request the message not be sent in MIME format.

We recommend that you use the `preamble.txt` file so that those who read MIME messages coming from your GroupWise system and who lack MIME-compliant mail readers can understand why they cannot read the message and can take corrective action.

If you choose to modify the `preamble.txt` file, be aware of the following considerations:

- The maximum file size is 1024 bytes (1 KB)
- This file is read by the GWIA when the GWIA starts, so if you change the file, you must restart the GWIA.

The GWIA's gateway folder also contains a `preamble.all` file. The `preamble.all` file includes the text of `preamble.txt` translated into several languages. If you anticipate that your users will be sending mail to non-English speaking users, you might want to copy the appropriate language sections from the `preamble.all` file to the preamble.txt file.

The 1024-byte limit on the size of the `preamble.txt` file still applies, so ensure that the file does not exceed 1024 bytes.

Customizing MIME Content-Type Mappings

By default, the GroupWise client determines the MIME content-type and encoding for message attachments. If, for some reason, the GroupWise client cannot determine the appropriate MIME content-type and encoding for an attachment, the GWIA must determine the content-type and encoding.

The GWIA uses a `mimetype.cfg` file to map attachments to the appropriate MIME content types. Based on an attachment's content type, the GWIA encodes the attachment using quoted-printable, Base64, or BinHex. Generally, quoted-printable is used for text-based files, Base64 for application files, and BinHex for Macintosh files.

The `mimetype.cfg` file includes mappings for many standard files. If necessary, you can modify the file to include additional mappings. If an attachment is sent that does not have a mapping in the file, the GWIA chooses quoted-printable, BinHex, or Base64 encoding.

The `mimetype.cfg` file is also used for RFC-822 attachments, but UUencode or BinHex encoding is used regardless of the mapped content type.

The `mimetype.cfg` file is located in the *domain*`\wpgate\`*gwia* folder. The following sections provide information you need to know to modify the file:

- "Mapping Format" on page 304
- "File Organization" on page 305

Mapping Format

Each mapping entry in the file uses the following format:

```
content-type .ext|dtk-code|mac-ttttcccc [/parms] ["comment"]
```

Element	Description
content-type	The MIME content type to which the file type is being mapped (for example, text/plain). You can omit the content-type only if you use the /parms element to explicitly define the encoding scheme for the file type.
.ext|dtk-*code*|mac-*ttttcccc*	The .ext element, dtk-*code* element, and mac-*ttttcccc* element are mutually exclusive. Each entry contains only one of the elements. • **.ext:** The file type extension being mapped to the content type (such as `.txt`). • **dtk-*code*:** The detect code being mapped to the content type (for example, dtk-1126). GroupWise assigns a detect code to each attachment type. • **mac-*ttttcccc*:** The Macintosh file type and creator application being mapped to the content type (for example, mac-textmswd). The first four characters (*tttt*) are used for the file type. The last four characters (*cccc*) are used for the creator application. You can use ???? for the creator portion (mac-text????) to indicate a certain file type created by any application. You can use ???? in both portions (mac-????????) to match any file type created by any application.

Element	Description
/parms	Optional parameters that can be used to override the default encoding assigned to the MIME content type. Possible parameters are: ◆ /alternate ◆ /parallel ◆ /base64 ◆ /quoted-printable ◆ /quoted-printable-safe ◆ /uuencode ◆ /plain ◆ /binhex ◆ /nofixeol ◆ /force-*ext* ◆ /noconvert ◆ /apple-single ◆ /apple-double
"comment"	Optional content description

File Organization

The `mimetype.cfg` file contains the following four sections:

- [Parameter-Override]
- [Mac-Mappings]
- [Detect-Mappings]
- [Extension-Mappings]

[Parameter-Override]

The `[Parameter-override]` section takes priority over other sections. You can use this section to force the encoding scheme for certain file types. This section also contains defaults for sending various kinds of multipart messages. This is how the GWIA knows to put attachments into MIME Alternate/Parallel multiparts.

[Mac-Mappings]

The `[Mac-mappings]` section defines mappings for Macintosh file attachments. The following is a sample entry:

```
application/msword mac-wdbnmswd "Word for Macintosh"
```

Macintosh files have a type and creator associated with them. The first four characters are used for the type and the last four characters are used for the creator application.

In the above example, the type is `wdbn` and the creator application is `mswd`. When a user attaches a Macintosh file to a message, the GWIA uses the appropriate entry in the `[Map-mappings]` section to map the file to a MIME content type and then encode the file according to the assigned encoding

scheme. Unless otherwise specified by the /parms element, BinHex 4.0 is used for the encoding. The following example shows how you can use the /parms element to change the encoding from the default (BinHex) to Base64:

```
application/msword mac-wdbnmswd /base64 "Word for Macintosh"
```

If necessary, you can use `????` for the creator portion (`mac-text????`) to indicate a certain file type created by any application. Or, you can use `????` in both portions (`mac-????????`) to match any file type created by any application. For example:

```
application/octet-stream mac-???????? /base64 "Mac Files"
```

This causes all Macintosh files to be encoded using Base64 rather than BinHex.

[Detect-Mappings]

GroupWise attempts to assign each attachment a detect code based on the attachment's file type. The `[Detect-mappings]` section defines the mappings based on these detect codes. The following is a sample entry:

```
application/msword dtk-1000 "Microsoft Word 4"
```

The GWIA uses the detect code to map to a MIME content type and then encode the file according to the assigned encoding scheme. If there is no mapping specified or if the file type cannot be determined, one of the other mapping methods, such as Extension-Mappings, are used. The detect codes associated with attachments are GroupWise internal codes and cannot be changed.

[Extension-Mappings]

If a mapping could not be made based on the entries in the `[Mac-mappings]` and `[Detect-mappings]` section, the GWIA uses the `[Extension-mappings]` section. The `[Extension-mappings]` section defines mappings based on the attachment's file extension. The following is a sample entry:

```
application/pdf .pdf
```

31 Configuring POP3/IMAP4 Services

The Post Office Protocol 3 (POP3) and the Internet Message Access Protocol 4 (IMAP4) are standard messaging protocols for the Internet. The GroupWise GWIA can function as a POP3 or an IMAP server, allowing access to the GroupWise domain database and message store. With POP3 or IMAP server functionality enabled, GroupWise users can download their messages from GroupWise to any POP3/IMAP4-compliant Internet email client. To send messages, POP3/IMAP4 clients can identify the GWIA as their SMTP server.

NOTE: Internal IMAP clients can connect directly to the POA, rather than connecting through the GWIA. For more information, see “Supporting IMAP Clients” on page 147. Direct connection provides faster access for internal IMAP clients.

Enabling POP3/IMAP4 Services

By default, POP3 service and IMAP4 service are not enabled.

To enable the POP3 service of the IMAP4 service:

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **POP3/IMAP4** tab.
3. To enable POP3, fill in the following fields:

   Enable POP3 Service: Allow POP3 downloads from a GroupWise mailbox. It corresponds with the GWIA’s --pop3 switch.

   Number of Threads for POP3 Connections: The POP3 threads setting lets you specify the number of connections for POP3 download requests. The default is 10 threads. This setting corresponds with the GWIA’s --pt switch.

   Number of Threads for POP3 SSL Connections: Specify the maximum number of threads you want the GWIA to use for secure POP3 connections. This setting corresponds with the GWIA’s --sslpt switch.

   Enable Intruder Detection: Configure the GWIA to log POP3 email clients in through the POA so that the POA’s intruder detection can take effect, if it has been configured in the GroupWise Admin console (Post Office object > **Client Settings > Enable Intruder Detection**). This setting corresponds with the GWIA’s --popintruderdetect switch.

   Do Not Publish GroupWise Information on an Initial POP3 Connection: This option suppresses the GroupWise information that the GWIA typically responds with when contacted by a POP client. It is enabled by default. This setting corresponds with the GWIA’s --nopopversion switch.

4. To enable IMAP4, fill in the following fields:

   Enable IMAP4 Service: Allow IMAP4 downloads and management of GroupWise messages. It corresponds with the GWIA’s --imap4 switch.

   Number of Threads for IMAP4 Connections: The IMAP4 threads setting lets you specify the number of connections for IMAP4 requests. The default is 10 threads. This setting corresponds with the GWIA’s --it switch.

Number of Threads for IMAP4 SSL Connections: Specify the maximum number of threads you want the GWIA to use for secure IMAP4 connections. This setting corresponds with the GWIA's --sslit switch.

Maximum Number of Items to Read: Specify in thousands the maximum number of items that you want the GWIA to download at one time. By default, the GWIA downloads 4,000 items at a time. For example, specify 5 to download 5,000 items at a time. The higher the setting, the more memory the GWIA uses to process a single folder. This setting corresponds with the GWIA's --imapreadlimit switch. See also the --imapreadnew switch.

Do Not Publish GroupWise Information on an Initial IMAP4 Connection: This option suppresses the GroupWise information that the GWIA typically responds with when contacted by an IMAP client. It is enabled by default. This setting corresponds with the GWIA's --noimapversion switch.

5 Click **Save**, then click **Close** to return to the main Admin console window.

The Post Office Agent (POA) can also be configured to support IMAP connections. You could offer IMAP services internally through the POA to provide faster response time for internal users. For more information, see "Supporting IMAP Clients" on page 147. However, IMAP is primarily available on the POA to support several third-party applications that communicate with the POA using IMAP, while the IMAP services provided by the GWIA provide the standard IMAP access used by users across the Internet.

Configuring Post Office Links

To function as a POP3/IMAP4 server, the GWIA requires access to each post office that contains mailboxes that will be accessed by a POP3/IMAP4 client. Post office links are modified on the Domain object of the domain that owns the post offices.

1 In the GroupWise Admin console, browse to and click the name of a domain.

2 Click **Post Office Links**, then click the name of the post office.

3 Edit the post office link as needed, then click **OK**.

Giving POP3 or IMAP4 Access Rights to Users

Access to POP3/IMAP4 services is determined by the class of service in which they are a member. By default, all users are members of the default class of service, which gives them POP3 and IMAP4 access.

If you changed the default class of service to exclude POP3 or IMAP4 access rights, or if you defined additional classes of services that do not provide POP3 or IMAP4 access rights, you might want to evaluate your currently defined classes of service to ensure that they provide the appropriate POP3 or IMAP4 access. For details, see "Controlling User Access to the Internet" on page 279.

Setting Up an Email Client for POP3/IMAP4 Services

With the GWIA set up as a POP3 and/or IMAP4 server, you can configure users' email clients to download messages from GroupWise mailboxes.

Most email clients are configured differently. However, all Internet clients need to know the following information:

- **POP3/IMAP4 Server:** The DNS hostname or IP address of the GWIA.

- **Login Name:** The user's GroupWise user name. For POP3 clients, there are several user name login options you can use to control how the GWIA handles the user's messages. For example, you can limit how many messages are downloaded each session. For more information, see "User Name Login Options" on page 309.
- **Password:** The user's existing GroupWise mailbox password. POP3/IMAP4 services requires users to have passwords assigned to their mailboxes.

User Name Login Options

With POP3 clients, users can add the options listed in the table below to the login name (GroupWise user name) to control management of their mailbox messages. If used, these options override the POP3 settings assigned through the user's class of service. See "Creating a Class of Service" on page 281.

Login options are appended to the user name with a colon character (:) between the user name and the switches:

Syntax: user_name:switch

Example: `User1:v=1`

You can combine options by stringing them together after the user name and the colon without any spaces between the options:

Syntax: user_name:switch1switch2

Example: `User1:v=1sdl=10`

The syntax for the user name options is not case sensitive. Login options are not required. If you do not want to include any login options, just enter the user name in the text box, or following the USER command if you are using a Telnet application as your POP3 client.

Option	Explanation	Example
v=*number between 1-31*	The v option defines the POP3 client's view number. If multiple POP3 clients access the same GroupWise mailbox, each client must use a different view number in order to see a fresh mailbox. For example, if two POP3 clients access a mailbox and the first client downloads the unread messages, the second client cannot download the messages unless it is using a different view number than the first client. If this option is not used, the default value is 1.	*User_Name*:v=1
d	The d option deletes the messages from the GroupWise mailbox after they have been downloaded to the POP3 client.	*User_Name*:d
p	The p option purges the messages from the GroupWise mailbox after they have been downloaded to the POP3 client.	*User_Name*:p
t=*1-1000*	The t option defines the download period, starting with the current day. For example, if you specify 14, then only messages that are 14 days old or newer are downloaded. If this option is not used, the default value is 30 days.	*User_Name*:t=14
n	The n option downloads messages in RFC-822 format rather than the default MIME format.	*User_Name*:N

Option	Explanation	Example
m	The m option downloads messages in MIME format. This is the default.	*User_Name*:M
s	The s option presets the file size when the STAT command is executed. If the user mailbox contains a lot of messages or large messages, it can take a long time to calculate the file size. With this option, the STAT command always reports an artificial file size of 1, which can save time.	*User_Name*:S
l=*1-1000*	The l option limits the number of messages to download for each POP3 session. For example, if you want to limit the number of messages to 10, you enter l=10. If this option is not used, the default value is 100 messages.	*User_Name*:L=10

32 Monitoring the GWIA

You can monitor the operation of the GWIA by using several different diagnostic tools. Each provides important and helpful information about the status of the GWIA and how it is currently functioning. Choose from the titles listed below to learn more about how to monitor the operations of the GWIA.

Using the GWIA Console

You can use the GWIA console to monitor the GWIA. You cannot use the GWIA console to change any of the GWIA's settings. Changes must be made through the GroupWise Admin console or the startup file.

Setting Up the GWIA Console

The web-based GWIA console is set up automatically when you install the GWIA, either as part of creating a new domain or when you install the GWIA on a non-domain server. You can optionally protect the GWIA console with a user name and password, or use an SSL connection between your web browser and the GWIA.

1 In the GroupWise Admin console, browse to and click the GWIA.

2 Click the **GroupWise** tab, then click **Agent Settings**, and locate the **HTTP** section.

3 (Conditional) If you want to use an SSL connection for the GWIA console, which provides optimum security, select **Enabled** or **Required** in the **HTTP SSL** drop-down list.

   - **Enabled:** If the GWIA is configured with a valid SSL certificate, the GWIA console uses SSL. If a valid SSL certificate is not available, the GWIA still provides the GWIA console, but without a secure SSL connection.
   - **Required:** The GWIA does not support the GWIA console unless a valid SSL certificate has been provided.

   For additional instructions about using SSL connections, see "Server Certificates and SSL Encryption" on page 695.

4 If you want to limit access to the GWIA console, fill in the **HTTP User Name** and **HTTP Password** fields.

   Unless you are using SSL, do not use a user name that is synchronized from an LDAP directory (such as NetIQ eDirectory or Microsoft Active Directory). This is because the information passes over the non-secure connection between your web browser and the agent. If you are using SSL, the user name is encrypted and therefore secure.

5 Click **Save**, then click **Close** to return to the main Admin console window.

6 Continue with Accessing the GWIA Console.

Accessing the GWIA Console

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **General** tab, then click **Launch GWIA Console**.

TIP: To access the GWIA console directly from your web browser, provide the URL where the GWIA is located by supplying the network address and port number. For example:

`http://gwia_server_address:9850`

Using GWIA Log Files

Error messages and other information about GWIA functioning are written to log files and can be displayed in the GWIA console. Log files can provide a wealth of information for resolving problems with GWIA functioning or message flow. This section covers the following subjects to help you get the most from GWIA log files:

Locating GWIA Log Files

The default location of the GWIA log files varies by platform:

Linux:	`/var/log/novell/groupwise/gwia.`*`domain`*
Windows:	*`domain`*`\wpgate\`*`gwia`*`\000.prc`

You can change the location where the GWIA creates its log files in the GroupWise Admin console and the GWIA configuration file (`gwia.cfg`).

Configuring GWIA Log Settings and Switches

When installing or troubleshooting the GWIA, a logging level of Verbose can be useful. However, when the GWIA is running smoothly, you can set the logging level down to Normal to conserve disk space occupied by log files.

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **GroupWise** tab, then click **Log Settings**.
3. Set the desired settings for logging.

   Log File Path: Browse to and select the folder where you want this GWIA to store its log files.

   Logging Level: Select the amount of data displayed on the GWIA agent console and written to the GWIA log file.

   - **Off:** Turns off disk logging and sets the logging level for the GWIA to its default. Logging information is still displayed on the GWIA agent console.
   - **Normal:** Displays only the essential information suitable for a smoothly running GWIA.
   - **Verbose:** Displays the essential information, plus additional information that can be helpful for troubleshooting.
   - **Diagnostic:** Turns on **Extensive Logging Options** and **SOAP Logging Options** on the GWIA console Log Settings page.

Maximum Log File Age: Specifies how many days to keep GWIA log files on disk. The default is 30 days.

Maximum Log Disk Space: Sets the maximum amount of disk space for all GWIA log files. When the specified disk space is consumed, the GWIA deletes existing log files, starting with the oldest. The default is 100 MB. The maximum allowable setting is 1000 MB (1 GB).

Corresponding Startup Switches: You can also use the --log, --loglevel, --logdays, and --logmax switches in the GWIA startup file to configure logging.

Viewing and Searching Log Files

You can view the contents of the GWIA log file in the GWIA console.

1. In the GWIA console, click **Log Files**.
2. To view a log file, select the log file, then click **View Events**.
3. To search for a specific string, select the log files to search, specify the string in the **Events Containing** field, then click **View Events**.

   TIP: To search all log files, select **Select All**.

4. To create a new log file, click **Cycle Log**.

Using GroupWise Monitor

GroupWise Monitor is a monitoring and management tool that allows you to monitor GroupWise agents from any location where you are connected to the Internet and have access to a web browser. In addition, GroupWise Monitor can notify you when agent problems arise.

For installation and setup instructions, see "Setting Up GroupWise Monitor" in the *GroupWise 18 Installation Guide*. For usage instructions, see Part XVII, "Monitor," on page 637.

Using Micro Focus Remote Manager

When GroupWise agents are running on Micro Focus Open Enterprise Server (OES), you can use Micro Focus Remote Manager to monitor them. For more information, see the *Micro Focus Remote Manager Administration Guide*.

Using an SNMP Management Console

You can monitor the GroupWise agents from SNMP management and monitoring programs. When properly configured, the GroupWise agents send SNMP traps to network management consoles for display along with other SNMP monitored programs.

Although the GroupWise agents are SNMP-enabled by default, the server where the GroupWise agents are installed must be properly configured to support SNMP, and the agents must also be properly configured. To set up SNMP services, complete the following tasks:

- "Setting Up SNMP Services for the GWIA" on page 314
- "Copying and Compiling the GWIA MIB File" on page 315
- "Configuring the GWIA for SNMP Monitoring" on page 315

Setting Up SNMP Services for the GWIA

Select the instructions for the platform where the GWIA runs:

- "Linux: Setting Up SNMP Services for the GWIA" on page 314
- "Windows: Setting Up SNMP Services for the GWIA" on page 314

Linux: Setting Up SNMP Services for the GWIA

The Linux GroupWise agents are compatible with NET-SNMP. An older version of SNMP called UCD-SNMP cannot be used with the Linux GroupWise agents. NET-SNMP comes with OES, but it does not come with SLES. If you are using SLES, you must update to NET-SNMP in order to use SNMP to monitor the Linux GroupWise agents.

1. Ensure you are logged in as root.
2. If NET-SNMP is not already set up on your Linux server, use the following command to configure SNMP:

   ```
   snmpconf -g basic_setup
   ```

   The `snmpconf` command creates the `snmpd.conf` file in one of the following folders, depending on your version of Linux:

   ```
   /usr/share/snmp
   /usr/local/share/snmp
   ~/.snmp
   ```

3. Locate the `snmpd.conf` file on your Linux server.
4. In a text editor, open the `snmpd.conf` file and add or uncomment the following lines:

   ```
   dlmod Gwsnmp /opt/novell/groupwise/agents/lib/libgwsnmp.so

   export LD_LIBRARY_PATH=/opt/novell/groupwise/agents/lib

   export MIBDIRS=/usr/share/snmp/mibs:/opt/novell/groupwise/agents/mibs

   export MIBS=ALL
   ```

5. Save the `snmpd.conf` file and exit the text editor.
6. Restart the SNMP daemon (snmpd) to put the changes into effect.

   IMPORTANT: Ensure that the SNMP daemon always starts before the POA starts.

Skip to "Copying and Compiling the GWIA MIB File" on page 315.

Windows: Setting Up SNMP Services for the GWIA

SNMP support is automatically installed along with the GroupWise agents. SNMP support is provided for up to instances of each GroupWise agent on the same Windows server. Upon startup, each instance of a GroupWise agent is dynamically assigned a row in its SNMP table. View the contents of the agent MIB for a description of the SNMP variables in the table.

On some versions of Windows Server, the SNMP Service is not included during the initial operating system installation. The SNMP Service can be added either before or after the GroupWise agents are installed on the Windows server.

Continue with Copying and Compiling the GWIA MIB File.

Copying and Compiling the GWIA MIB File

An SNMP-enabled GroupWise agent returns information contained in a Management Information Base (MIB). The MIB is an ASCII data structure that defines the information gathered. It also defines the properties that can be monitored and managed on the SNMP-enabled GroupWise agent.

Before you can monitor an SNMP-enabled GroupWise agent, you must compile the agent MIB file using your SNMP management program. GroupWise agent MIB files are located in the `/agents/mibs` folder in your GroupWise software installation.

The MIB file contains all the Trap, Set, and Get variables used for communication between the GroupWise agent and the SNMP management console. The Trap variables provide warnings that point to current and potential problems. The Set variables allow you to configure portions of the application while it is still running. The Get variables display the current status of different processes of the application.

1. Copy the agent MIB file to the location required by your SNMP management program.
2. Compile or import the agent MIB file as required by your SNMP management program.

Continue with Configuring the GWIA for SNMP Monitoring.

Configuring the GWIA for SNMP Monitoring

In order for SNMP monitoring programs to monitor the a GroupWise agent, the GroupWise agent must be configured with an SNMP community string.

1. In the GroupWise Admin console, browse to and click the GroupWise agent object.
2. Click the **Agent Settings** tab, then locate the **SNMP Community "Get" String** field.
3. Provide your system SNMP community "Get" string, then click **OK**.
4. Configure the SNMP Service with the same community "Get" string.
5. Restart the GroupWise agent.

   The GroupWise agent should now be visible to your SNMP monitoring program.

Assigning Users to Receive GWIA Warning and Error Messages

You can select GroupWise users to receive warning and error messages issued by the GWIA. Whenever the agent issues a warning or error, these users receive a message in their mailboxes. You can specify one or more GWIA administrators.

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **GroupWise** tab, then click **Administrators**.
3. Click **Add**, select one or more GroupWise users or groups, then click **OK**.
4. Ensure that **Operator** is selected as the Administrator Role.
5. Click **Save**, then click **Close** to return to the main Admin console window.

Stopping the GWIA

The GWIA can be stopped in the same ways as the other GroupWise agents. See “Working with the GroupWise Agents” in the *GroupWise 18 Installation Guide*.

In addition, you can use the following methods that do not apply to the other GroupWise agent:

- “Using a Mail Message” on page 316
- “Using a Shutdown File” on page 316

Using a Mail Message

The GWIA can be stopped by sending a shutdown message to the GWIA. In order to shut down the program with a message, the user sending the message must be defined as an operator for the GWIA. This prevents unauthorized users from shutting down the GWIA. For information about defining a user as an operator, see “Assigning Users to Receive GWIA Warning and Error Messages” on page 315.

The message to shut down the GWIA must be addressed to the GWIA, not a non-GroupWise domain. The syntax for the `To` line is:

`gwia``:shutdown`

Replace *gwia* with the name of the GWIA object.

Using a Shutdown File

The GWIA can also be stopped by placing a file named `shutdown` in the *`domain`*`/wpgate/`*`gwia`*`/000.prc` folder. When the GWIA sees this file, it deletes the file and shuts down.

33 Optimizing the GWIA

The following sections provide information about some of the methods you can use to optimize the speed and reliability of the GroupWise GWIA:

Optimizing Send/Receive Threads

The GWIA uses sending and receiving threads to process incoming and outgoing messages. The more threads you make available, the more messages the GWIA can process concurrently. However, threads place a demand on the server's resources. Too many threads can monopolize memory and CPU utilization.

Ensure that you balance your processing speed requirements with the other applications running on the same server as the GWIA.

For information about adjusting the SMTP sending and receiving threads, see "Configuring Basic SMTP/MIME Settings" on page 293.

Increasing Polling Time

Incoming and outgoing messages are stored in priority queues. The GWIA polls these queues and then forwards the messages for distribution. The **Time** option lets you control how often the GWIA polls these queuing folders. Ensure that you balance polling time requirements with the other applications running on the same server as the GWIA.

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **GroupWise** tab, then click **Time Settings**.
3. Modify the following settings:

   Idle Sleep Duration: Select the time, in seconds, you want the GWIA to idle after it has processed its queues. A low setting, such as 5 seconds, speeds up processing but requires more resources. A higher setting slows down the GWIA but requires fewer resources by reducing the number of network polling scans. The default is 10 seconds.

   Snap Shot Interval: The **Snap Shot Interval** is a sliding interval you can use to monitor GWIA activity. For example, if the **Snap Shot Interval** remains at the default (10 minutes), the **Snap Shot** columns in the console display only the previous 10 minutes of activity.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Decreasing the Timeout Cycles

The GWIA has a series of switches that control its timeout settings. By decreasing the default time of the timeout cycles you might be able to slightly increase the GWIA speed. However, the timeout cycles do not place an extremely significant burden on the overall performance of the GWIA so the effect might be minimal. You should consider this option only after you have tried everything else.

For information about configuring the timeout settings in the GroupWise Admin console, see “Configuring the SMTP Timeout Settings” on page 299. For information about configuring the settings using startup switches, see “Timeouts” on page 341.

34 Using GWIA Startup Switches

You can override settings provided in the GroupWise Admin console by using startup switches in the GWIA startup file (`gwia.cfg`). The default location for the `gwia.cfg` file is in the `wpgate/gwia` subfolder in the domain folder.

When you create a domain and install the GWIA, an initial `gwia.cfg` file is created. This initial file includes the --home startup switch set to the `wpgate/gwia` subfolder.

Startup switches specified on the command line override those in the `gwia.cfg` file. Startup switches in the `gwia.cfg` file override corresponding settings in the GroupWise Admin console. You can view the `gwia.cfg` file from the Configuration page of the GWIA console.

Alphabetical List of Switches

Primary configuration settings are available in the GroupWise Admin console. Secondary configuration settings are not available in the GroupWise Admin console and can be set only using switches in the `gwia.cfg` file.

Switch starts with: a b c d e f g h i j k l m n o p q r s t u v w x y z

Linux GWIA	Windows GWIA	GroupWise Admin Console Settings
--aql	/aql	**SMTP/MIME > Address Handling > Sender's Address Format**
--aqor --noaqor	/aqor /noaqor	**SMTP/MIME > Address Handling > Place Domain and Post Office Qualifiers on Right of Address**
--ari	/ari	N/A
--attachmsg --noattachmsg	/attachmsg /noattachmsg	N/A
--badmsg	/badmsg	**SMTP/MIME > Undeliverables > Undeliverable or Problem Message**
--blockrulegenmsg	/blockrulegenmsg	N/A
--certfile	/certfile	**GroupWise > SSL Settings > Certificate File**
--cluster	/cluster	N/A
--dbchar822	/dbchar822	N/A
--defaultcharset	/defaultcharset	N/A
--dhome	/dhome	**Server Folders > Settings > SMTP Queues Directory**
--dhparm	/dhparm	N/A
--delayedmsgnotification --nodelayedmsgnotification	/delayedmsgnotification /nodelayedmsgnotification	**SMTP/MIME > Settings**

Linux GWIA	Windows GWIA	GroupWise Admin Console Settings
--dia --nodia	/dia /nodia	SMTP/MIME > Address Handling > Ignore GroupWise Internet Addressing
N/A	/dialpass	SMTP/MIME > Dial-Up Settings > Password
N/A	/dialuser	SMTP/MIME > Dial-Up Settings > Username
-disallowauthrelay	/disallowauthrelay	N/A
--displaylastfirst --nodisplaylastfirst	/displaylastfirst /nodisplaylastfirst	SMTP/MIME > Address Handling > Display Fullname as Lastname, Firstname
--dontreplaceunderscore --replaceunderscore	/dontreplaceunderscore /replaceunderscore	SMTP/MIME > Address Handling > Do Not Replace Underscores with Spaces
--dsn --nodsn	/dsn /nodsn	SMTP/MIME > ESMTP Settings > Enable Delivery Status Notification (DSN)
--dsnage	/dsnage	SMTP/MIME > ESMTP Settings > DSN Hold Age
--etrnhost	/etrnhost	SMTP/MIME > Dial-Up Settings > ETRN Host
--etrnqueue	/etrnqueue	SMTP/MIME > Dial-Up Settings > ETRN Queue
--fd822	/fd822	SMTP/MIME > Address Handling > Non-GroupWIse Domain for RFC-822 Replies
--fdmime	/fdmime	SMTP/MIME > Address Handling > Non-GroupWIse Domain for MIME Replies
--flatfwd --noflatfwd	/flatfwd /noflatfwd	SMTP/MIME > Message Formatting > Enable Flat Forwarding
--force7bitout --noforce7bitout	/force7bitout /noforce7bitout	SMTP/MIME > Settings > Use 7 Bit Encoding for All Outbound Messages
--forceinboundauth	/forceinboundauth	N/A
--forceoutboundauth	/forceoutboundauth	N/A
--fut	/fut	SMTP/MIME > Undeliverables > Forward Undeliverable Inbound Messages
--group --nogroup	/group /nogroup	SMTP/MIME > Address Handling > Expand Groups on Incoming Messages
--hn	/hn	SMTP/MIME > Settings > Hostname/DNS Record “A Record” Name
--home	/home	N/A
--httppassword	/httppassword	GroupWise > Optional Gateway Settings > HTTP Password
--httpport	/httpport	GroupWise > Network Address > HTTP Port
--httprefresh	/httprefresh	N/A
--httpssl	/httpssl	GroupWise > Network Address > HTTP SSL

Linux GWIA	Windows GWIA	GroupWise Admin Console Settings
--httpuser	/httpuser	GroupWise > Optional Gateway Settings > HTTP User Name
--imap4	/imap4	POP3/IMAP4 > Settings > Enable IMAP4 Service
--imapport	/imapport	GroupWise > Network Address > IMAP Port
--imapreadlimit	/imapreadlimit	POP3/IMAP4 > Settings > Maximum Number of Items to Read
--imapreadnew	/imapreadnew	N/A
--imapsport	/imapsport	GroupWise > Network Address > IMAP SSL Port
--imapssl	/imapssl	GroupWise > Network Address > IMAP SSL
--imip--noimip	/imip /noimip	SMTP/MIME > Settings > Enable iCal Service
--ip	/ip	GroupWise > Network Address > Bind Exclusively to TCP/IP Address
--ipa	/ipa	N/A
--ipp	/ipp	N/A
--iso88591is	/iso88591is	N/A
--it	/it	POP3/IMAP4 > Settings > Number of Threads for IMAP4 Connections
--keepsendgroups --nokeepsendgroups	/keepsendgroups /nokeepsendgroups	SMTP/MIME > Address Handling > Retain Distribution Lists on Outgoing Messages
--keyfile	/keyfile	GroupWise > SSL Settings > SSL Key File
--keypasswd	/keypasswd	GroupWise > SSL Settings > Password
--killthreads --nokillthreads	/killthreads /nokillthreads	SMTP/MIME > Settings > Kill Threads on Exit or Restart
--koi8	/koi8	N/A
--ldap	/ldap	LDAP > Settings > Enable LDAP Service
--ldapcntxt	/ldapcntxt	LDAP > Settings > LDAP Context
--ldapipaddr	/ldapipaddr	N/A
--ldapport	/ldapport	GroupWise > Network Address > LDAP Port
--ldappwd	/ldappwd	N/A
--ldaprefcntxt	/ldaprefcntxt	LDAP > Settings > LDAP Context
--ldaprefurl	/ldaprefurl	LDAP > Settings > LDAP Referral URL
--ldapserverport	/ldapserverport	GroupWise > Network Address > LDAP Port
--ldapserversslport	/ldapserversslport	GroupWise > Network Address > LDAP SSL Port

Linux GWIA	Windows GWIA	GroupWise Admin Console Settings
--ldapssl --noldapssl	/ldapssl /noldapssl	GroupWise > Network Address > LDAP SSL
--ldapthrd	/ldapthrd	LDAP > Settings > Number of LDAP Threads
--ldapuser	/ldapuser	N/A
--log	/log	GroupWise > Log Settings > Log File Path
--logdays	/logdays	GroupWise > Log Settings > Max Log File Age
--loglevel	/loglevel	GroupWise > Log Settings > Log Level
--logmax	/logmax	GroupWise > Log Settings > Max Log Disk Space
--maxdeferhours	/maxdeferhours	SMTP/MIME > Settings > Maximum Number of Hours to Retry a Deferred Message
--mbcount	/mbcount	SMTP/MIME > Security Settings > Enable Mailbomb Protection and Mailbomb Threshold
--mbtime	/mbtime	SMTP/MIME > Security Settings > Enable Mailbomb Protection and Mailbomb Threshold
--mh	/mh	SMTP/MIME > Settings > Relay Host for Outbound Messages
--mime	/mime	SMTP/MIME > Message Formatting > Default Message Encoding: MIME
--msgdeferinterval	/msgdeferinterval	SMTP/MIME > Settings > Intervals to Retry a Deferred Message
--msstu	/msstu	N/A
--mudas	/mudas	SMTP/MIME > Undeliverables > Amount of Original Message to Return to Sender When Message Is Undeliverable
--nasoq	/nasoq	N/A
--nickgroup	/nickgroup	N/A
--noesmtp	/noesmtp	N/A
--noimapversion	/noimapversion	SMTP/MIME > POP3/IMAP4 > Settings > Do Not Publish GroupWise Information on an Initial IMAP4 Connection
--noiso2022 --iso2022	/noiso2022 /iso2022	N/A
--nomappriority --mappriority	/nomappriority /mappriority	SMTP/MIME > Message Formatting > Disable Mapping X-Priority Fields
--nopopversion	/nopopversion	SMTP/MIME > POP3/IMAP4 > Settings > Do Not Publish GroupWise Information on an Initial POP3 Connection

Linux GWIA	Windows GWIA	GroupWise Admin Console Settings
--nosmtpversion --smtpversion	/nosmtpversion /smtpversion	**SMTP/MIME > Settings > Do Not Display GroupWise Information on an Initial SMTP Connection**
--nosnmp	/nosnmp	N/A
--notfamiliar --familiar	/notfamiliar /familiar	N/A
--nqpmt	/nqpmt	**SMTP/MIME > Message Formatting > Enable Quoted Printed Message Text Line Wrapping**
--p	/p	**SMTP/MIME > Settings > Scan Cycle for Send Directory**
--pop3 --nopop3	/pop3 /nopop3	**POP3/IMAP4 > Settings > Enable POP3 Service**
--popintruderdetect	/popintruderdetect	**POP3/IMAP4 > Settings > Enable Intruder Detection**
--popport	/popport	**GroupWise > Network Address > POP Port**
--popsport	/popsport	**GroupWise > Network Address > POP SSL Port**
--popssl	/popssl	**GroupWise > Network Address > POP SSL**
--pt	--pt	**POP3/IMAP4 > Settings > Number of Threads for POP3**
--rbl	/rbl	**Access Control > Blacklists > Blacklist Addresses**
--rd	/rd	**SMTP/MIME > Settings > Number of SMTP Receive Threads**
--realmailfrom --norealmailfrom	/realmailfrom /norealmailfrom	**SMTP/MIME > Address Handling > Use GroupWise User Address as Mail From: for Rule Generated Messages**
--rejbs	/rejbs	**SMTP/MIME > Security Settings > Reject Mail If Sender's Identity Cannot Be Verified**
--relayaddsignature	/relayaddsignature	**SMTP/MIME > Message Formatting > Apply Global Signature to Relay Messages**
--rt	/rt	**SMTP/MIME > Message Formatting > Number of Inbound Conversion Threads**
--sd	/sd	**SMTP/MIME > Settings > Number of SMTP Send Threads**
--show	N/A	N/A
--smtp	/smtp	**SMTP-MIME > Settings > Enable SMTP**
--smtphome	/smtphome	**Server Folders > Settings > Advanced > SMTP Service Queues Directory**
--smtpport	/smtpport	**GroupWise > Network Address > SMTP Port**
--smtpssl	/smtpssl	**GroupWise > Network Address > SMTP SSL**

Linux GWIA	Windows GWIA	GroupWise Admin Console Settings
--sslciphersuite	/sslciphersuite	N/A
--sslit	/sslit	POP3/IMAP4 > Settings > Number of Threads for IMAP4 SSL Connections
--ssloption	/ssloption	N/A
--sslpt	/sslpt	POP3/IMAP4 > Settings > Number of Threads for POP3 SSL Connections
--st	/st	SMTP/MIME > Message Formatting > Number of Outbound Conversion Threads
--tc	/tc	SMTP/MIME > Timeouts > Commands
--td	/td	SMTP/MIME > Timeouts > Data
--te	/te	SMTP/MIME > Timeouts > Connection Establishment
--tg	/tg	SMTP/MIME > Timeouts > Greeting
--tr	/tr	SMTP/MIME > Timeouts > TCP Read
--tt	/tt	SMTP/MIME > Timeouts > Connection Termination
--usedialup	/usedialup	SMTP/MIME > Dial-Up Settings > Enable Dial-Up
--uueaa	/uueaa	SMTP/MIME > Message Formatting > UUEncode All Message Attachments
--work	/work	Server Directories > Settings > Conversion Directory
--wrap	/wrap	SMTP/MIME > Message Formatting > Line Wrap Length for Message Text on Outbound Mail
--xspam	/xspam	SMTP/MIME > Junk Mail

Required Switches

The following switches point the GWIA to the GWIA's folder. They are assigned their initial value during installation.

--dhome
--hn
--home

@config_file_name

Specifies the location of the GWIA configuration file (`gwia.cfg`). The `gwia.cfg` file is created in the `/` *`domain_folder`*`/wpgate/`*`gwia`* folder. The `gwi.cfg` file includes the --home switch.

--dhome

Points to the SMTP service work area. This is normally the same as the GWIA folder (`/` *`domain_folder`*`/wpgate/`*`gwia`*).

Syntax: --dhome *path_name*

Linux Example: --dhome /gwsystem/provo1/gwia

Windows Example: /dhome=c:\gwsystem\provo2\gwia

--hn

Specifies the hostname that is displayed when someone connects to your GWIA using a Telnet session. You should enter the hostname assigned to you by your Internet service provider.

Syntax: --hn *host_name*

Example: --hn gwia.novell.com

This switch is required only under certain circumstances. Normally, the GWIA gets the information from another source and does not need this switch. If you receive a message that the --hn switch is required, you must use the switch.

--home

Specifies the GWIA home folder (`/`*`domain_folder`*`/wpgate/`*`gwia`*), where the GWIA can find its databases, input/output queues, and configuration files. There is no default location. You must use this switch in order to start the GWIA.

Syntax: --home *gateway_folder*

Linux Example: --home /gwsystem/provo1/gwia

Windows Example: /home-j:\headq\wpgate\gwia

If you specify a UNC path with the --home switch when you run the GWIA as a Windows service, you must configure the GWIA service to run under a specific Windows user account. If you specify a local folder or a mapped drive, you can configure the GWIA service to run under the local system account.

Environment Switches

The following switches configure GWIA environment settings such as working folders, clustering support, and SNMP support.

--cluster
--ip
--ipa
--nosnmp
--smtphome

--work

--cluster

Informs the GWIA that it is running in a cluster. A clustered GWIA automatically binds to the IP address configured for the GWIA object even if the **Bind Exclusively to TCP/IP Address** option is not selected on the GWIA **Agent Settings** tab in the GroupWise Admin console. This prevents unintended connections to other IP addresses, such as the loopback address or the node's physical IP address. For information about clustering the GWIA, see "Clustering" in the *GroupWise 18 Interoperability Guide*.

Syntax: --cluster

--ip

Binds the GWIA to the specified IP address so that, on a server with multiple IP addresses, the GWIA uses only the specified IP address.

Syntax: --ip *address*

Example: --ip 172.16.5.18

--ipa

Specifies the IP address (or hostname) of a GroupWise POA that the GWIA can use to resolve IP addresses of other POAs in the system. This replaces the need to configure post office links for the GWIA in the GroupWise Admin console (Domain object > **Post Office Links**).

If you have established a GroupWise name server (`ngwnameserver`), you can use it. See "Simplifying Client Access with a GroupWise Name Server" on page 145.

Syntax: --ipa *address*

Example: --ipa ngwnameserver

--ipp

Specifies the port number of a GroupWise POA that the GWIA can use to resolve IP addresses of other POAs in the system. This replaces the need to configure post office links for the GWIA in the GroupWise Admin console (Domain object > **Post Office Links**).

If you have established a GroupWise name server (`ngwnameserver`), you can use it. See "Simplifying Client Access with a GroupWise Name Server" on page 145.

Syntax: --ipp *port_number*

Example: --ipp 678

--nosnmp

Disables SNMP for the GWIA. The default is to have SNMP enabled. See "Using an SNMP Management Console" on page 313.

Syntax: --nosnmp

--smtphome

Specifies a secondary SMTP queues folder for inbound and outbound messages. This secondary folder can be helpful for troubleshooting by providing a way to trap messages before they are routed to the Internet. You can also use the secondary folder to run third-party utilities such as a virus scanner on Internet-bound messages.

The GWIA places all outbound messages in this secondary folder. The messages must then be moved manually (or by another application) to the primary SMTP queue's send folder (--dhome switch) before the GWIA routes them to the Internet.

Syntax: --smtphome *path*

Example: `--smtphome mail:\provo1\wpgate\gwia\smtp2`

--work

Sets the folder where the GWIA stores its temporary files. On Linux, the work folder is located in the domain by default. On Windows, it is not.

Linux:	*domain*`/wpgate/`*gwia*`/000.prc/gwwork`
Windows:	*c*`:\`*grpwise*`\`*gwia*

Syntax: --work *path_name*

Linux Example: --work /opt/novell/groupwise/tmp

Windows Example: /work -j:\tmp\work

--nasoq

By default, the GWIA sends the accounting file (`acct`) to users specified as accountants in the GroupWise Admin console (GWIA object > **GroupWise > Administrators**). The file is sent daily at midnight and any time the GWIA shuts down.

This switch configures the GWIA to send the acct file once daily at midnight, not each time the GWIA quits or is shut down.

Syntax: --nasoq

SMTP/MIME Switches

The following sections categorize and describe the switches that you can use to configure the GWIA's SMTP/MIME settings:

- "SMTP Enabled" on page 328
- "iCal Enabled" on page 328
- "Address Handling" on page 328
- "Message Formatting and Encoding" on page 333
- "Forwarded and Deferred Messages" on page 337
- "Extended SMTP" on page 338

- “Send/Receive Cycle and Threads” on page 339
- “Dial-Up Connections” on page 340
- “Timeouts” on page 341
- “Relay Host” on page 342
- “Host Authentication” on page 342
- “Undeliverable Message Handling” on page 343
- “Mailbomb and Spam Security” on page 344

SMTP Enabled

The following switches enable SMTP and suppress version information display.

--smtp
--nosmtpversion

--smtp

Enables the GWIA to process SMTP messages. See “Configuring Basic SMTP/MIME Settings” on page 293.

Syntax: --smtp

--nosmtpversion

Suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by another SMTP host or a telnet session.

Syntax: --nosmtpversion

iCal Enabled

The following switch enables iCal.

--imip

--imip

Converts outbound GroupWise Calendar items into MIME text/calendar iCal objects and converts incoming MIME text/calendar messages into GroupWise Calendar items.

Syntax: --imip

Address Handling

The following switches determine how the GWIA handles email addresses:

--aql
--aqor
--ari
--blockrulegenmsg

--dia
--displaylastfirst
--dontreplaceunderscore
--fd822
--fdmime
--group
--keepsendgroups
--msstu
--nomappriority
--notfamiliar
--realmailfrom

--aql

Determines the address qualification level. It specifies which GroupWise address components (domain.post_office.user) must be included as the user portion of a GroupWise user's outbound Internet address (userhost). Valid options are auto, userid, po, and domain.

This switch is valid only if your system is not configured to use Internet-style addressing. For more information, see Chapter 29, "Managing Internet Domains, Addressing, and Access," on page 273, Or you have configured the GWIA to ignore Internet-style addressing. For more information, see "Configuring How the GWIA Handles Email Addresses" on page 296.

Syntax: --aql *option*

Example: --aql po

Option	Description
auto	This option causes the gateway to include the addressing components required to make the user's address unique. If a user name is unique in a GroupWise system, the outbound address uses only the *user_name*. If the *post_office* or *domain.post_office* components are required to make the address unique, these components are also included in the outbound address. The auto option is the default.
userid	This option requires the gateway to include only the *user_name* in the outbound Internet address, even if the user name is not unique in the system. If a recipient replies to a user whose user name is not unique and no other qualifying information is provided, that reply cannot be delivered.
po	This option requires the gateway to include *post_office.user_name* in every outbound address, regardless of the uniqueness or non-uniqueness of the user name.
domain	This option requires the gateway to include the fully qualified GroupWise address (*domain.post office.user_name*) in every outbound address, regardless of the uniqueness or non-uniqueness of the user name. This option guarantees the uniqueness of every outbound Internet address, and ensures that any replies are delivered.

--aqor

The user part of a GroupWise user's outbound Internet address (*user@host*) can and sometimes must include the full Groupwise address (*domain.post_office.user_name@host*) in order to be unique. The --aqor switch configures the GWIA to move any GroupWise address components, except

the *user_name* component, to the right side of the address following the at sign (@). In this way, GroupWise addressing components become part of the host portion of the outbound Internet address. The --aql switch specifies which components are included.

For example, if the --aqor switch is used (in conjunction with the --aql-*domain* switch), Bob Thompson's fully qualified Internet address (`headquarters.advertising.bob@novell.com`) is resolved to `bob@advertising.headquarters.novell.com` for all outbound messages.

If the --aqor switch is used with the --aql-*po* switch, Bob's Internet address is resolved to `bob@advertising.novell.com` for all outbound messages.

If you use the --aqor switch to move GroupWise domain or post office names to be part of the host portion on the right side of the address, you must provide a way for the DNS server to identify the GroupWise names. You must either explicitly name all GroupWise post offices and domains in your system as individual MX Records, or you can create an MX Record with wildcard characters to represent all GroupWise post offices and domains. For information about creating MX Records, see details found in RFC #974.

For details about this setting, see "Configuring How the GWIA Handles Email Addresses" on page 296.

--ari

Enables or disables additional routing information that is put in the SMTP return address to facilitate replies. This switch might be needed in large systems with external GroupWise domains in which the external GroupWise users have not been configured in your local domain. Options include **Never** and **Always**. Most sites do not need to use this switch.

Syntax: --ari *never|always*

Example: --ari never

--blockrulegenmsg

In the GroupWise Admin console, you can control whether or not rule-generated messages are allowed to leave your GroupWise system by selecting or deselecting the **Rule-Generated Messages** options available in each class of service defined for the GWIA. This switch allows you to be specific in the types of rule-generated messages that are blocked.

Syntax: --blockrulegenmsg forward | reply | none | all

Example: --blockrulegenmsg forward

In order for this switch to take effect, senders must be in a class of service where rule-generated messages are allowed. For more information, see "Creating a Class of Service" on page 281.

--dia

GroupWise supports both Internet-style addressing (*user@host*) and GroupWise proprietary addressing (*user_name.post_office.domain*). By default, the GWIA uses Internet-style addressing. See "Configuring How the GWIA Handles Email Addresses" on page 296. You can use this switch to disable Internet-style addressing.

Syntax: --dia

--displaylastfirst

By default, users' display names are First Name Last Name. If you want users' display names to be Last Name First Name, you can use the --displaylastfirst switch. This forces the display name format to be Last Name First Name, regardless of the preferred address format.

Syntax: --displaylastfirst

--dontreplaceunderscore

By default, the GWIA accepts addresses of the format:

firstname_lastname@internet_domain_name

Even though this is not an address format that the GroupWise Admin console included in the Allowed Address Formats list in the GroupWise Admin console for configuring Internet addressing, you can use this switch to prevent this address format from being accepted by the GWIA. For more information, see "Allowed Address Formats" on page 276.

Syntax: --dontreplaceunderscore

--fd822

Specifies a return address for GroupWise replies. A message that has been received by a GroupWise user through the GWIA and is replied to has this return address form. These switches cause the GWIA to produce a return address of the form *foreign domain*.*type*:"*user host*." *Foreign domain* can be any foreign domain you have configured and linked to the GWIA.

You can use the same foreign domain name for both the --fd822 switch and the --fdmime switch. You can specify multiple foreign domain and kind pairs by placing them in quotes. If multiple foreign domain and kind pairs are used, the first domain/kind pair is the return address for replies to messages received through the GWIA. The second domain/kind pair is checked to see what message format is used for old replies in the system. Up to four pairs can be specified with an 80-character limit.

This switch lets you change your foreign domain names in your GroupWise system and still have replies work. For example, if your foreign domain is called *faraway* and you added a foreign domain called Internet, you could use --fd822-"internet.nonmime smtp.nonmime." This causes replies to have a return address of internet.nonmime.:"*user@host*." The GWIA would also recognize *faraway*. This switch also lets you migrate from one foreign domain to another.

Most administrators do not need to use this switch.

Syntax: --fd822 *foreign_domain.type*

Example: --fd822 Internet.nonmime

--fdmime

Specifies a return address for GroupWise replies. A message that has been received by a GroupWise user through the GWIA and is replied to has this return address form. These switches cause the GWIA to produce a return address of the form *foreign_domain*.*type*:"*user host*." *Foreign_domain* can be any foreign domain you have configured and linked to the GWIA. *Type* can be either mime or nonmime.

You can use the same foreign domain name for both the --fd822 switch and the --fdmime switch.

You can specify multiple foreign domain and kind pairs by placing them in quotes. If multiple foreign domain and kind pairs are used, the first domain/kind pair is the return address for replies to messages received through the GWIA. The second domain/kind pair is checked to see what message format is used for old replies in the system. Up to four pairs can be specified with an 80-character limit.

This switch lets you change your foreign domain names in your GroupWise system and still have replies work. For example, if your foreign domain is called SMTP and you add a foreign domain called Internet, you can use --fdmime-"internet.mime smtp.mime." This causes replies to have a return address of internet.mime:"*user@host*." The GWIA also recognizes SMTP. This switch also lets you migrate from one foreign domain to another.

Most administrators do not need to use this switch.

Syntax: --fdmime *foreign_domain.type*

Example: --fdmime Internet.mime

--group

Turns on group expansion. By default, the GWIA does not expand groups, which means that recipients listed in groups do not receive incoming Internet messages that are addressed to groups.

Use this switch to expand groups into individual email addresses of the group members, so that the recipients in groups do receive incoming Internet messages addressed to groups. See “Configuring How the GWIA Handles Email Addresses” on page 296.

Syntax: --group

See also --nickgroup.

--keepsendgroups

When constructing the MIME for outgoing messages, discard all users that expanded out of system distribution lists. Instead include a reference to the distribution list. This results in a smaller MIME and Reply to All list for the recipient. This setting corresponds with the GWIA’s --keepsendgroups switch.

Syntax: --keepsendgroups

NOTE: If you retain groups on outgoing messages, Reply to All might not work unless you also enable inbound group expansion by using the --group switch.

--msstu

Replaces spaces with underscores (_) in the email address of the sender for outbound messages. For example, john smith becomes john_smith.

It does not replace spaces in the addresses of recipients.

Syntax: --msstu

--nickgroup

Turns on group expansion only for groups that have nicknames. By default, the GWIA does not expand groups, which means that recipients listed in groups do not receive incoming Internet messages that are addressed to groups. If you use the --group switch, the GWIA expands all groups.

Use this switch to expand only nicknamed groups. This means that recipients listed in nicknamed groups do receive incoming Internet messages that are addressed to the nickname of the group, but they do not receive incoming Internet messages that are addressed to groups that do not have nicknames. For information about nicknames, see “Managing User Email Addresses” on page 471. See also “Configuring How the GWIA Handles Email Addresses” on page 296.

Syntax: --nickgroup

See also --group.

--nomappriority

Disables the function of mapping an x-priority **MIME** field to a GroupWise priority for the message. By default, the GWIA maps x-priority 1 and 2 messages as high priority, x-priority 3 messages as normal priority, and x-priority 4 and 5 as low priority in GroupWise.

Syntax: --nomappriority

--notfamiliar

Configures the GWIA to not include the user’s familiar name, or display name, in the **From** field of the message’s MIME header. In other words, the **From** field is *address* rather than "*familiar_name*" *address*.

Syntax: --notfamiliar

--realmailfrom

Configures the GWIA to use the real user in the **Mail From** field instead of having auto-forwards come from Postmaster and auto-replies come from Mailer-Daemon.

Syntax: --realmailfrom

Message Formatting and Encoding

The following switches determine how the GWIA formats and encodes inbound and outbound email messages:

--attachmsg
--dbchar822
--charsetconfidencelevel
--defaultcharset
--defaultnonmimecharset
--force7bitout
--iso88591is
--koi8
--mime
--noiso2022

--noqpmt
--relayaddsignature
--rt
--st
--uueaa
--wrap

For more information, see "MIME Encoding" on page 88.

--attachmsg

Configures the GWIA to maintain the original format of any file type attachment.

Syntax: --attachmsg

--charsetconfidencelevel

Sets the confidence level at which you want the GWIA to use the detected character set rather than the default character set when no character set is specified. The GWIA tries to detect the character set based on the presence or absence of certain characters in the text. The default confidence level is 25, meaning that if the detection process returns a confidence level of 25 or above, the GWIA uses the detected character set, but if the confidence level is less than 25, the GWIA uses the default character set. Valid values range from 0 to 100.

Syntax: --charsetconfidencelevel *number*

Example: --charsetconfidencelevel 35

--dbchar822

Configures the GWIA to map inbound non-MIME messages to another character set that you specify. The mapped character set must be an Asian (double-byte) character set.

Syntax: `--dbchar822 charset`

Example: --dbchar822 shift_jis

--defaultcharset

Specifies what character set to use if no character set is specified in an incoming MIME-encoded message.

Syntax: --defaultcharset *charset*

Example: --defaultcharset iso-8859-1

--defaultnonmimecharset

Specifies what character set to use if no character set is specified in an incoming message that is not MIME encoded. The default is US_ASCII.

Syntax: --defaultnonmimecharset *charset*

Example: --defaultnonmimecharset iso-8859-1

--force7bitout

By default, the GWIA uses 8-bit MIME encoding for any outbound messages that are HTML-formatted or that contain 8-bit characters. If, after connecting with the receiving SMTP host, the GWIA discovers that the receiving SMTP host cannot handle 8-bit MIME encoded messages, the GWIA converts the messages to 7-bit encoding.

You can use the --force7bitout switch to force the GWIA to use 7-bit encoding and not attempt to use 8 bit MIME encoding. You should use this option if you are using a relay host that does not support 8-bit MIME encoding. See "Configuring Basic SMTP/MIME Settings" on page 293.

Syntax: --force7bitout

--iso88591is

Configures the GWIA to map inbound MIME ISO-8859-1 messages to another character set that you specify.

Syntax: --iso88591is *charset*

Example: --iso88591is big5

--koi8

Configures the GWIA to map all outbound MIME messages to the KOI8 (Russian) character set.

Syntax: --koi8

--mime

Configures the GWIA to send outbound messages in MIME format rather than in RFC-822 format. If you've defined an RFC-822 non-GroupWise domain, users can still send RFC-822 formatted messages by using the RFC-822 domain in the address string when sending messages. For more information, see "Adding External Users to the GroupWise Address Book" on page 78.

Removing the switch corresponds to enabling the Default Message Encoding: Basic RFC-822 setting in the GroupWise Admin console. See "Determining Format Options for Messages" on page 298.

Syntax: --mime

--noiso2022

Configures the GWIA to not use ISO-2022 character sets. ISO-2022 character sets provide 7-bit encoding for Asian character sets.

Syntax: --noiso2022

--nqpmt

Disables quoted printable message text for outbound messages. If this switch is turned on, messages are sent with Base64 MIME encoding, unless all the text is US-ASCII. If you use this switch you need to review the setting for the --wrap switch to ensure that message text wraps correctly. See "Determining Format Options for Messages" on page 298.

Syntax: --nqpmt

--relayaddsignature

Appends the global signature to messages that are relayed through your GroupWise system (for example, messages from POP and IMAP clients) in addition to messages that originate within your GroupWise system. See “Adding a Global Signature to Users’ Messages” on page 460.

Syntax: --relayaddsignature

--rt

Specifies the maximum number of threads that the GWIA uses when converting inbound messages from MIME or RFC-822 format to the GroupWise message format. The default setting is 4. The lowest valid setting is 1. There is no upper limit, but the larger the number of threads, the more resources are used, perhaps with little benefit unless a very large amount of data needs to be processed in a very small amount of time. See “Determining Format Options for Messages” on page 298.

Multiple threading allows for more than one receive process to be running concurrently. A receive request is assigned to a single thread and is processed by that thread. If you anticipate heavy inbound message traffic, you can increase the number of threads to enhance the speed and performance of the GWIA. The number of threads is limited only by the memory resources of your server.

Syntax: --rt

--st

Specifies the maximum number of threads that the GWIA uses when converting outbound messages from GroupWise message format to MIME or RFC-822 format. The default setting is 4. The lowest valid setting is 1. There is no upper limit, but the larger the number of threads, the more resources are used, perhaps with little benefit unless a very large amount of data needs to be processed in a very small amount of time. See “Determining Format Options for Messages” on page 298.

Multiple threading allows for more than one send process to be running concurrently. A send request is assigned to a single thread and is processed by that thread. If you anticipate heavy outbound message traffic, you can increase the number of threads to enhance the speed and performance of the GWIA. The number of threads is limited only by the memory resources of your server.

Syntax: --st

--uueaa

Forces the GWIA to UUencode any ASCII text files attached to outbound RFC-822 formatted messages. This switch applies only if the --mime switch is not used. Without this switch, the GWIA includes the text as part of the message body. See “Determining Format Options for Messages” on page 298.

Syntax: --uueaa

--wrap

Sets the line length for outbound messages that do not use quoted printable or Base64 MIME encoding. This is important if the recipient's email system requires a certain line length. See "Determining Format Options for Messages" on page 298.

Syntax: --wrap *line_length*

Example: --wrap 72

Forwarded and Deferred Messages

The following switches configure how the GWIA handles forwarded and deferred messages:

--flatfwd
--delayedmsgnotification
--maxdeferhours
--msgdeferinterval

--flatfwd

Automatically strips out the empty message that is created when a message is forwarded without adding text, and retains the original sender of the message, rather than showing the user who forwarded it. This facilitates users forwarding messages from GroupWise to other email accounts. Messages arrive in the other accounts showing the original senders, not the users who forwarded the messages from GroupWise.

Syntax: --flatfwd

--delayedmsgnotification

Provides a notification message to users whose email messages cannot be immediately sent out across the Internet. This provides more noticeable notification to users than manually checking the Properties page of the sent item to see whether it has been sent.

Syntax: --delayedmsgnotification

See "Configuring Basic SMTP/MIME Settings" on page 293.

--maxdeferhours

Specifies the number of hours after which the GWIA stops trying to send deferred messages. The default is 96 hours, or four days. You might prefer to receive an undeliverable notification sooner, perhaps in as little as 5 hours. A deferred message is any message that can't be sent because of a temporary problem (host down, MX record not found, and so on). See "Configuring Basic SMTP/MIME Settings" on page 293.

Syntax: --maxdeferhours *hours*

Example: --maxdeferhours 48

--msgdeferinterval

Specify in a comma-delimited list the number of minutes after which the GWIA retries sending deferred messages. The default is 20, 20, 20, 240. The GWIA interprets this list as follows: It retries 20 minutes after the initial send, 20 minutes after the first retry, 20 minutes after the second retry, and 240 minutes (4 hours) after the third retry. You might prefer for the fourth retry to occur sooner, perhaps in only 2 hours.

Thereafter, it retries according to the last retry interval until the number of hours specified in the **Maximum Number of Hours to Retry a Deferred Message** field is reached. You can provide additional retry intervals as needed. It is the last retry interval that repeats until the maximum number of hours is reached. See "Configuring Basic SMTP/MIME Settings" on page 293.

Syntax: --msgdeferinterval *minutes*,*minutes*...,*minutes*

Example: --msgdeferinterval 10,10,10,120

Extended SMTP

The following switches configure the GWIA's Extended SMTP (ESMTP) settings:

--noesmtp
--dsn
--dsnage

--noesmtp

Disables ESMTP support in the GWIA.

Syntax: --noesmtp

--dsn

Enables Delivery Status Notification (DSN). The GWIA requests status notifications for outgoing messages and supplies status notifications for incoming messages. This requires the external email system to also support Delivery Status Notification. Currently, notification consists of two delivery statuses: successful and unsuccessful. See "Using Extended SMTP (ESMTP) Options" on page 295.

Syntax: --dsn

--dsnage

The --dsnage switch specifies the number of days that the GWIA retains information about the external sender so that status updates can be delivered to him or her. For example, the default DSN age causes the sender information to be retained for 4 days. If the GWIA does not receive delivery status notification from the GroupWise recipient's Post Office Agent (POA) within that time period, it deletes the sender information and the sender does not receive any delivery status notification. See "Using Extended SMTP (ESMTP) Options" on page 295.

Syntax: --dsnage

Send/Receive Cycle and Threads

The following switches configure the GWIA's SMTP send/receive cycle and threads:

--p
--rd
--sd
--killthreads
--smtpport

--p

Specifies how often, in seconds, the GWIA polls for outbound messages. The default,10 seconds, causes the GWIA to poll the outbound message folder every 10 seconds. See "Configuring Basic SMTP/MIME Settings" on page 293.

Syntax: --p *seconds*

Example: --p 5

--rd

Specifies the maximum number of threads used for processing SMTP receive requests (inbound messages). Each thread is equivalent to one connection. The default is 16 threads. Setting the receive threads to 0 stops messages from being received through the GWIA. There is no upper limit, but the larger the number of threads, the more resources are used, perhaps with little benefit. See Section 30, "Configuring SMTP/MIME Services," on page 293.

Syntax: --rd *number_of_threads*

Example: --rd 20

--sd

Specifies the maximum number of threads used for processing SMTP send requests (outbound messages). Each thread is equivalent to one connection. The default is 8 threads. Setting the send threads to 0 stops messages from being sent through the GWIA. There is no upper limit, but the larger the number of threads, the more resources are used, perhaps with little benefit. See "Configuring Basic SMTP/MIME Settings" on page 293.

Syntax: --sd *number_of_threads*

Example: --sd 12

--killthreads

Configures the GWIA to quickly terminate any active send/receive threads when it restarts.

Syntax: --killthreads

--smtpport (Linux only)

Changes the SMTP listen port from the default of 25. Use this switch only if the GWIA is receiving messages only from SMTP hosts that can be configured to connect to GWIA on a specified port.

Syntax: --smtpport

Example: --smtpport 2525

Dial-Up Connections

SMTP dial-up services can be used when you don't require a permanent connection to the Internet and want to periodically check for mail messages queued for processing. The following switches can be used when configuring dial-up services.

--usedialup
--etrnhost
--etrnqueue
/dialuser (Windows only)
/dialpass (Windows only)

--usedialup

Enables SMTP dial-up services.

Syntax: --usedialup

--etrnhost

Specifies the IP address or DNS hostname of the mail server where your mail account resides at your Internet Service Provider. You should obtain this address from your Internet Service Provider.

Syntax: --etrnhost *address*

Example: --etrnhost 172.16.5.18

--etrnqueue

Specifies your email domain as provided by your Internet Service Provider.

Syntax: --etrnqueue *email_domain*

Example: --etrnqueue novell.com

/dialuser (Windows Only)

Specifies the RAS Security user if you are using a Windows Remote Access Server (RAS) and the GWIA is not running on the same server as the RAS.

Syntax: /dialuser-*user_name*

Example: /dialuser-rasuser

/dialpass (Windows Only)

Specifies the RAS Security user’s password if you are using a Windows Remote Access Server (RAS) and the GWIA is not running on the same server as the RAS.

Syntax: /dialpass-*password*

Example: /dialpass-raspassword

Timeouts

The following switches specify how long SMTP services waits to receive data that it can process. After the time expires, the GWIA might give a TCP read/write error. Leave these switches at the default setting unless you are experiencing a problem with communication.

--tc
--td
--te
--tg
--tr
--tt

--tc

Specifies how long the program waits for an SMTP command. The default is 2 minutes.

Syntax: --tc *minutes*

Example: --tc 3

--td

Specifies how long the program waits for data from the receiving host. The default is 5 minutes.

Syntax: --td *minutes*

Example: --td 2

--te

Specifies how long the program waits for the receiving host to establish a connection. The default is 5 minutes.

Syntax: --te *minutes*

Example: --te 2

--tg

Specifies how long the program waits for the initial greeting from the receiving host. The default is 3 minutes.

Syntax: --tg *minutes*

Example: --tg 2

--tr

Specifies how long the program waits for a TCP read. The default is 10 minutes.

Syntax: --tr *minutes*

Example: --tr 2

--tt

Specifies how long the program waits for the receiving host to terminate the connection. The default is 5 minutes.

Syntax: --tt *minutes*

Example: --tt 2

Relay Host

The following switch configures whether or not the GWIA uses a relay host.

--mh

--mh

Specifies the IP address or DNS hostname of one or more relay hosts that you want the GWIA to use for outbound messages. Use a space to separate multiple relay hosts in a list.

The relay host can be part of your network or can reside at the Internet service provider's site. This switch is typically used in firewall integration if you want one server, the specified relay host, to route all mail. See "Configuring Basic SMTP/MIME Settings" on page 293.

Syntax: --mh *address*

Example: --mh 172.16.5.18

Host Authentication

The GWIA supports SMTP host authentication for both inbound and outbound message traffic. The following switches are used with inbound and outbound authentication:

--forceinboundauth
--forceoutboundauth

--forceinboundauth

Ensures that the GWIA accepts messages only from remote SMTP hosts that use the AUTH LOGIN authentication method to provide a valid GroupWise user name and password. The remote SMTP hosts can use any valid GroupWise user name and password. However, for security reasons, we recommend that you create a dedicated GroupWise user account for remote SMTP host authentication.

Syntax: --forceinboundauth

NOTE: Using the --forceinboundauth switch overrides the Prevent Message Relaying setting for the GWIA in the GroupWise Admin console for POP and IMAP users. To completely prevent message relaying when using the --forceinboundauth switch, you must also specify the --disallowauthrelay switch.

--forceoutboundauth

Ensures that the GWIA sends messages only to remote SMTP hosts that are included in a `gwauth.cfg` text file. The remote SMTP hosts must support the AUTH LOGIN authentication method.

The `gwauth.cfg` file must reside in the *`domain`*`\wpgate\`*`gwia`* folder and use the following format:

`domain_name authuser authpassword`

For example:

```
smtp.novell.com remotehost novell
```

You can define multiple hosts in the file. Ensure that you include a hard return after the last entry.

If you use this switch, you need to include your GWIA as an entry in the `gwauth.cfg` file to enable status messages to be returned to GroupWise users. You can use any GroupWise user name and password for your GWIA's authentication credentials. However, for security reasons, we recommend that you create a dedicated GroupWise user account for your GWIA.

Syntax: --forceoutboundauth

Undeliverable Message Handling

The following switches determine how the GWIA handles undeliverable messages:

--badmsg
--fut
--mudas

--badmsg

Specifies where to send problem messages. Problem messages can be placed in the GWIA problem folder (`gwprob`), they can be sent to the postmaster, or they can be sent to both or neither. The values for this switch are move, send, both, and neither.

The move option specifies to place problem messages in the `gwprob` folder for the GWIA. The send option specifies to send the message as an attachment to the GWIA postmaster defined in the GroupWise Admin console (GWIA object > **GroupWise > Administrators**). The both option specifies to move the message to `gwprob` and send it to the postmaster. The neither option specifies to discard problem messages. The default when no switch is specified is move. See "Determining What to Do with Undeliverable Messages" on page 300.

Syntax: --badmsg move|send|both|neither

Example: --badmsg both

--fut

Forwards undeliverable messages to the specified host. See "Determining What to Do with Undeliverable Messages" on page 300.

Syntax: --fut *host*

Example: --fut novell.com

--mudas

Controls how much of the original message is sent back when a message is undeliverable. By default, only 2 KB of the original message is sent back. The value is specified in KB (8=8KB). See "Determining What to Do with Undeliverable Messages" on page 300.

Syntax: --mudas *KB*

Example: --mudas 16

Mailbomb and Spam Security

Multiple unsolicited messages (sometimes called a *mailbomb* or *spam*) from the Internet can potentially harm your GroupWise messaging environment. At the least, it can be annoying to your users. You can use the following switches to help protect your GroupWise system from malicious, accidental, and annoying attacks:

--disallowauthrelay
--mbcount
--mbtime
--rejbs
--xspam
--rbl

--disallowauthrelay

Prevents spammers from using GroupWise accounts to authenticate to the GWIA and using it as a relay host for their spam. It has no effect on normal GroupWise account usage in a GroupWise client or WebAccess. However, it does prevent users who access their GroupWise mailboxes from a POP or IMAP client from sending messages to users outside of the GroupWise system, because the GWIA identifies this activity as relaying.

Syntax: --disallowauthrelay

--mbcount

Sets the number of messages that can be received from a single IP address in a given number of seconds before the GWIA denies access to its GroupWise system. It provides a form of system security to protect your system from mailbombs.

For example, with --mbcount set to 25 and --mbtime set to 60 seconds, if these limits are exceeded then the sender's IP address is blocked from sending any more messages for the remainder of that 60 second window. The IP address of the sender is also displayed in the GWIA console. You can permanently restrict access to your system by that IP address through settings on the Access Control

tab in the GroupWise Admin console (GWIA object > **Access Control**). By default, the mailbomb feature is turned off. To enable this feature, you must specify a value for mailbomb count and mailbomb time. See "Mailbomb (Spam) Protection" on page 287.

Syntax: --mbcount-*number*

Example: --mbcount 25

--mbtime

Specifies the mailbomb time limit in seconds. This switch works with the --mbcount switch to block access to your GroupWise system from unsolicited inundations of email. The default value is 10 seconds. See "Mailbomb (Spam) Protection" on page 287.

Syntax: --mbtime *seconds*

Example: --mbtime 60

--rejbs

Prevents delivery of messages if the sender's host is not authentic. When this switch is used, the GWIA refuses messages from a host if a DNS reverse lookup shows that a PTR record does not exist for the IP address of the sender's host. See "Mailbomb (Spam) Protection" on page 287.

If this switch is not used, the GWIA accepts messages from any host, but displays a warning if the initiating host is not authentic.

Syntax: --rejbs

--xspam

Flags messages to be handled by the client Junk Mail Handling feature if they contain an x-spam-flag:yes in the MIME header. See "Customized Spam Identification" on page 288.

Syntax: --xspam

--rbl

Lets you define the addresses of blacklist sites (free or fee-based) you want the GWIA to check for blacklisted hosts. If a host is included in a site's blacklist, the GWIA does not accept messages from it.

Syntax: --rbl bl.spamcop.net

This switch corresponds to the Blacklist Addresses list (GWIA object > **Access Control > Blacklists**). For details about this setting, see "Real-Time Blacklists" on page 285.

POP3 Switches

The following optional startup switches that can be used to configure the GWIA's POP3 service:

--nopopversion
--pop3
--popintruderdetect
--popport

--popsport
--popssl
--pt
--sslpt

--nopopversion

Suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by a POP client.

Syntax: --nopopversion

--pop3

Enables POP3 client access to GroupWise mailboxes through the GWIA. See "Enabling POP3/IMAP4 Services" on page 307.

Syntax: --pop3

--popintruderdetect

Configures the GWIA to log POP email clients in through the POA so that the POA's intruder detection can take effect, if intruder has been configured in the GroupWise Admin console (Post Office object > **Client Settings > Intruder Detection**).

Syntax: --popintruderdetect

--popport

By default, the GWIA listens for POP3 connections on port 110. This switch allows you to change the POP3 listen port.

Syntax: --popport *port_number*

Example: --popport 111

--popsport

By default, the GWIA listens for secure (SSL) POP3 connections on port 995. This switch allows you to change the POP3 SSL listen port.

Syntax: --popsport *port_number*

Example: --popsport 996

--popssl

Disables, enables, or requires secure (SSL) connections between POP3 clients and the GWIA. See "Securing Internet Access with SSL Connections to the GWIA" on page 271.

Syntax: --popssl *enabled*|*disabled*|*required*

Example: --popssl required

Option	Description
enabled	The POP3 client determines whether an SSL connection or non-SSL connection is used. By default, the GWIA listens for SSL connections on port 995 and non-SSL connections on port 110. You can use the --popsport and --popport switches to change these ports.
required	The GWIA forces SSL connections on port 995 and port 110. Non-SSL connections are denied. You can use the --popsport and --popport switches to change these ports.
disabled	The GWIA listens for connections only on port 110, and the connections are not secure. You can use the --popport switch to change this port.

--pt

Specifies the maximum number of threads to be used for POP3 connections. The default number is 10. You are limited only by the memory resources of your server. See "Enabling POP3/IMAP4 Services" on page 307.

Syntax: --pt *number_of_threads*

Example: --pt 15

--sslpt

Specify the maximum number of threads you want the GWIA to use for secure POP3 connections. You are limited only by the memory resources of your server. See "Enabling POP3/IMAP4 Services" on page 307.

Syntax: --sslpt *number_of_threads*

Example: --sslpt 15

IMAP4 Switches

The following optional startup switches that can be used to configure the GWIA's IMAP4 service:

--imap4
--imapport
--imapreadlimit
--imapreadnew
--imapsport
--imapssl
--it
--noimapversion
--sslit

--imap4

Enables IMAP4 client access to GroupWise mailboxes through the GWIA. See "Enabling POP3/IMAP4 Services" on page 307.

Syntax: --imap4

--imapport

By default, the GWIA listens for IMAP4 connections on port 143. This switch allows you to change the IMAP4 listen port.

Syntax: --imapport *port_number*

Example: --imapport 144

--imapreadlimit

By default, the GWIA downloads a maximum of 4,000 items at a time. This switch allows you to specify, in thousands, the maximum number of items you want the GWIA to download. For example, specifying 10 indicates 10,000.

Syntax: --imapreadlimit *number_of_items*

Example: --imapreadlimit 10

--imapreadnew

By default, the GWIA reads items in a folder from the oldest to the newest. As a result, if a folder contains more items than are allowed by the /imapreadlimit setting, users receive the older items but not the newer items. Enable this switch so that the GWIA reads items from the newest to the oldest. This ensures that users receive all their new items in a timely manner.

Syntax: --imapreadnew

--imapsport

By default, the GWIA listens for secure (SSL) IMAP4 connections on port 993. This switch allows you to change the IMAP4 SSL listen port.

Syntax: --imapsport *port_number*

Example: --imapsport 994

--imapssl

Disables, enables, or requires secure (SSL) connections between IMAP4 clients and the GWIA. See "Securing Internet Access with SSL Connections to the GWIA" on page 271.

Syntax: --IMAP4ssl *enabled*|*disabled*|*required*

Example: --popssl required

Option	Description
enabled	The IMAP4 client determines whether an SSL connection or non-SSL connection is used. By default, the GWIA listens for SSL connections on port 993 and non-SSL connections on port 143. You can use the --imapsport and --imapport switches to change these ports.
required	The GWIA forces SSL connections on port 993 and port 143. Non-SSL connections are denied. You can use the --imapsport and --imapport switches to change these ports.
disabled	The GWIA listens for connections only on port 143, and the connections are not secure. You can use the --imapport switch to change this port.

--it

Specifies the maximum number of threads to be used for IMAP4 connections. The default number is 10. You are limited only by the memory resources of your server. See "Enabling POP3/IMAP4 Services" on page 307.

Syntax: --it *number_of_threads*

Example: --it 15

--noimapversion

Suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by an IMAP client.

Syntax: --noimapversion

--sslit

Specify the maximum number of threads you want the GWIA to use for secure IMAP4 connections. You are limited only by the memory resources of your server. See "Enabling POP3/IMAP4 Services" on page 307.

Syntax: --sslit *number_of_threads*

Example: --sslit 15

SSL Switches

The GWIA can use SSL to enable secure SMTP, POP, IMAP, and HTTP connections. The following switches can be used to 1) specify the server certificate file, key file, and key file password required for SSL and 2) enable or disable SSL for SMTP, POP, IMAP, and HTTP connections. See "Securing Internet Access with SSL Connections to the GWIA" on page 271.

--certfile
--dhparm
--keyfile
--keypasswd
--smtpssl
--httpssl

--popssl
--imapssl
--ldapssl
--sslciphersuite
--ssloption

--certfile

Specifies the server certificate file to use. The file must be in Base64/PEM or PFX format. If the file is not in the same folder as the GWIA program, specify the full path.

Syntax: --certfile *file_name*

Example: --certfile \\server1\sys\server1.crt

--dhparm

Specifies a Diffie-Hellman cipher parameters file used for SSL/TLS to replace the default parameters set by GroupWise. GroupWise uses default Diffie-Hellman parameters of 2048 bits to generate the DH key. A valid DH parameter is in PEM format.

	Linux	Windows
Syntax:	--dhparm *directory/pemfile*	/dhparm *directory/pemfile*
Example:	--dhparm /var/tmp/dh.pem	/dhparm C:\temp\dh.pem

--keyfile

Specifies the private key file to use. The key file is required if the certificate file does not contain the key. If the certificate file contains the key, do not use this switch. When specifying a file name, use the full path if the file is not in the same folder as the GWIA program.

Syntax: --keyfile *file_name*

Example: --keyfile \\server1\sys\server1.key

--keypasswd

Specifies the private key password. If the key does not require a password, do not use this switch.

Syntax: --keypasswd *password*

Example: --keypasswd novell

--smtpssl

Enables the GWIA to use a secure connection to other SMTP hosts. The SMTP host must also be enabled to use SSL or TLS (Transport Layer Security); if it is not, a non-secure connection is used. Valid settings are enabled and disabled.

Syntax: --smtpssl *setting*

Example: --smtpssl enabled

--httpssl

Enables the GWIA to use a secure connection to a web browser being used to display the GWIA console. The web browser must also be enabled to use SSL; if it is not, a non-secure connection is used. Valid settings are enabled and disabled.

Syntax: --httpssl *setting*

Example: --httpssl enabled

--popssl

Disables, enables, or requires secure (SSL) connections between POP3 clients and the GWIA.

Syntax: --popssl *enabled*|*disabled*|*required*

Example: --popssl required

Option	Description
enabled	The POP3 client determines whether an SSL connection or non-SSL connection is used. By default, the GWIA listens for SSL connections on port 995 and non-SSL connections on port 110. You can use the --popsport and --popport switches to change these ports.
required	The GWIA forces SSL connections on port 995 and port 110. Non-SSL connections are denied. You can use the --popsport and --popport switches to change these ports.
disabled	The GWIA listens for connections only on port 110, and the connections are not secure. You can use the --popport switch to change this port.

--imapssl

Disables, enables, or requires secure (SSL) connections between IMAP4 clients and the GWIA.

Syntax: --IMAP4ssl *enabled*|*disabled*|*required*

Example: --popssl required

Option	Description
enabled	The IMAP4 client determines whether an SSL connection or non-SSL connection is used. By default, the GWIA listens for SSL connections on port 993 and non-SSL connections on port 143. You can use the --imapsport and --imapport switches to change these ports.
required	The GWIA forces SSL connections on port 993 and port 143. Non-SSL connections are denied. You can use the --imapsport and --imapport switches to change these ports.
disabled	The GWIA listens for connections only on port 143, and the connections are not secure. You can use the /imapport switch to change this port.

/ldapssl

Configures the GWIA to use a secure (SSL) connection with an LDAP server. For more information about why the GWIA would need to connect to an LDAP server, see “Log File Switches” on page 355

Syntax: /ldapssl

--sslciphersuite

Sets the SSL cipher suites used by the Archive Agent, the Messaging Agent, and Messenger clients. The cipher list must be in OpenSSL format. For more information on OpenSSL format, see Cipher List Format (https://www.openssl.org/docs/apps/ciphers.html#CIPHER-LIST-FORMAT)

	Linux	Windows
Syntax:	--sslciphersuite *"setting"*	/sslciphersuite-*"setting"*
Example:	--sslciphersuite "HIGH:!AECDH:!EXP:@STRENGTH"	/sslciphersuite-"HIGH:!AECDH:!EXP:@STRENGTH"

--ssloption

Specify a specific SSL protocol to disable. By specifying SSL_OP_NO_TLSv1, GroupWise will disable TLSv1 support. Specify additional options by adding the SSL key work separated by a comma.

	Linux	Windows
Syntax:	--ssloption *SSL_protocol*	/ssloption *SSL_protocol*
Example:	--ssloption SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1	/ssloption SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1

LDAP Switches

The GWIA can perform GroupWise authentication of POP3/IMAP4 clients through an LDAP server and can also perform LDAP queries for GroupWise information.

The following sections describe the switches required to configure this functionality:

- "GroupWise Authentication Switches" on page 352
- "LDAP Query Switches" on page 353

GroupWise Authentication Switches

When a POP3/IMAP4 user attempts to access a GroupWise mailbox on a post office that has been configured for LDAP authentication, the GWIA connects to the post office's POA, which then connects to the LDAP server so that the LDAP server can authenticate the user.

This process works automatically if the GWIA's link to the post office is client/server (meaning that it communicates through TCP/IP to the post office's POA). If the GWIA is using a direct link to the post office folder rather than a client/server link to the post office's POA, the GWIA must communicate directly with the LDAP server rather communicate through the POA.

The following switches are used to provide the GWIA with the required LDAP server information:

--ldapipaddr
--ldapport
--ldapssl

--ldapuser
--ldappwd

--ldapipaddr

Specifies the IP address of the LDAP server through which GroupWise authentication takes place.

Syntax: --ldapipaddr *address*

Example: --ldapipaddr 172.16.5.18

--ldapport

Specifies the port number being used by the LDAP server. The standard non-SSL LDAP port number is 389. The standard SSL LDAP port number is 636.

Syntax: --ldapport *number*

Example: --ldapport 389

--ldapssl

Configures the GWIA to use a secure (SSL) connection with the LDAP server.

Syntax: --ldapssl

--ldapuser

Specifies a user that has rights to the LDAP folder. The user must have at least Read rights.

Syntax: --ldapuser *user_name*

Example: --ldapuser ldap

--ldappwd

Specifies the password of the user specified by the --ldapuser switch.

Syntax: --ldappwd *password*

Example: --ldappwd pwd1

LDAP Query Switches

The GWIA can function as an LDAP server, allowing LDAP queries for GroupWise user information contained in the folder. The following switches configure the GWIA as an LDAP server.

--ldap
--ldapthrd
--ldapcntxt
--ldaprefurl
--ldaprefcntxt
--ldapserverport
--ldapserversslport

--ldap

Enables the GWIA as an LDAP server.

Syntax: --ldap

--ldapthrd

Specifies the maximum number of threads the GWIA can use for processing LDAP queries. The default is 10.

Syntax: --ldapthrd *number*

Example: --ldapthrd 5

--ldapcntxt

Limits the folder context in which the LDAP server searches. For example, you could limit LDAP searches to a single Micro Focus organization container located under the United States country container.

If you restrict the LDAP context, you must ensure that users, when defining the folder in their email client, enter the same context (using the identical text you did) in the Search Base or Search Root field.

Syntax: --ldapcntxt "*context*"

Example: --ldapcntxt "O=Micro Focus,C=US"

--ldaprefurl

Defines a secondary LDAP server to which you can refer an LDAP query if the query fails to find a user or address in your GroupWise system. For this option to work, the requesting web browser must be able to track referral URLs.

Syntax: --ldaprefurl *url*

Example: --ldapurl ldap://ldap.provider.com

--ldaprefcntxt

Limits the folder context in which the secondary (referral) LDAP server searches.

Syntax: --ldaprefcntxt "*context*"

Example: --ldaprefcntxt "O=Micro Focus,C=US"

--ldapserverport

Changes the LDAP listen port from the default of 389.

Syntax: --ldapserverport *port_number*

Example: --ldapserverport 390

--ldapserversslport

Changes the LDAP SSL listen port from the default of 636.

Syntax: --ldapserversslport *port_number*

Example: --ldapserversslport 637

Log File Switches

The following switches control how the GWIA uses the log file. The log file keeps a record of all GWIA activity. See "Using GWIA Log Files" on page 312.

--log
--logdays
--loglevel
--logmax

--log

The default location for GWIA log files varies by platform:

Linux:	`/var/log/novell/groupwise/`*`domain_name`*`.gwia`
Windows	*`domain`*`\wpgate\gwia\000.prc`

The log files are named after the month, day, and log number for that date (*mmdd*`gwia.`*nn*).You can use the --log switch to redirect the log files to a different location.

Syntax: --log-*log_file_folder*

Linux Example: --log /opt/novell/groupwise/agents/log

Windows Example: --log-c:\log\gwia

--logdays

Specifies how many days to keep GWIA log files on disk. The default log file age is 30 days. The valid range is from 1 to 350 days.

Syntax: --logdays *days*

Example: --logdays 5

--loglevel

Defines the amount of information to record in log files.

The values are:

- Diagnostic
- Verbose

* Normal (Default)
* Off

Syntax: --loglevel *level*

Example: --loglevel verbose

--logmax

Controls the maximum amount of disk space for all log files. The amount of disk space each log file consumes is added together to determine the total amount of disk space used. When the limit is reached, the GWIA deletes the existing log files, starting with the oldest one. The default is 102400 (100 MB). The maximum allowable setting is 102400000 (1 GB). Specify 0 (zero) for unlimited disk space.

Syntax: --logmax *KB*

Example: --logmax 512

Console Switches (HTTP)

The following switches enable the HTTP console and control its configuration settings. The console enables you to monitor the GWIA through a web browser. For more information, see "Using the GWIA Console" on page 311.

--httpport
--httpuser
--httppassword
--httprefresh
--httpssl

--httpport

Specifies the port where the GWIA listens for the console. The default port established during installation is 9850.

Syntax: --httpport *port_number*

Example: --httpport 9851

--httpuser

By default, any user who knows the GWIA's address and port (--httpport) can use the console. This switch adds security to the console by forcing users to log into the console using the specified user name. The --httppassword switch must also be used to establish the user password.

Syntax: --httpuser *user_name*

Example: --httpuser gwia

The *user_name* can be any arbitrary name.

--httppassword

Specifies the password that must be supplied along with the user name provided by --httpuser.

Syntax: --httppassword *password*

Example: --httppassword monitor

--httprefresh

By default, the GWIA refreshes the console information every 60 seconds. You can use this switch to override the default refresh interval.

Syntax: --httprefresh *seconds*

Example: --httprefresh 120

--httpssl

Enables the GWIA to use a secure connection to a web browser being used to display the GWIA console. The web browser must also be enabled to use SSL; if it is not, a non-secure connection is used. See "Securing Internet Access with SSL Connections to the GWIA" on page 271.

Syntax: --httpssl

Console Switches (Server)

The following switches apply to the GWIA server console:

--color
--help
--mono
--show

--color

Sets the default color of the GWIA console. The values range from 0-7.

Syntax: color-*0*|*1*|*2*|*3*|*4*|*5*|*6*|*7*

Example: --color 3

You can also change the color of the screen for a GWIA session. From the menu on the bottom of the console, select **Options**, then press the key for **Colors**.

--help

Displays the Help screen for the startup switches.

Syntax: --help

--mono

Runs the GWIA for a computer with a monochrome monitor.

Syntax: --mono

--show (Linux Only)

Starts the GWIA with a server console user interface.

By default, no user interface is provided for the agents on Linux. An agent that runs with a user interface cannot be managed in the GroupWise Admin console.

The --show startup switch can be used on the command line or in the `gwha.conf` file used by the GroupWise High Availability Service. It cannot be placed in the agent startup file.

Syntax: --show

The --show switch cannot be used in the GWIA startup file (`gwia.cfg`). However, if you want the GWIA to start with a user interface when you run the `grpwise` script or when the server reboots, you can configure the GroupWise High Availability service (gwha) to accomplish this. An agent that runs with a user interface cannot be managed in the GroupWise Admin console because it is not running as a service.

VII Document Viewer Agent

- Chapter 35, “Understanding Document Conversion,” on page 361
- Chapter 36, “Scaling Your DVA Installation,” on page 363
- Chapter 37, “Configuring the DVA,” on page 369
- Chapter 38, “Monitoring the DVA,” on page 373
- Chapter 39, “Optimizing the DVA,” on page 377
- Chapter 40, “Using DVA Startup Switches,” on page 379

For port number information, see “Document Viewer Agent Port Numbers” on page 729.

For detailed Linux-specific DVA information, see Appendix C, “Linux Basics for GroupWise Administration,” on page 735.

35 Understanding Document Conversion

The document files that users attach to messages are as varied as the combinations of document formats, tools, and users throughout the world. The Document Viewer Agent (DVA) accommodates multiple attachment formats by converting GroupWise attachments into HTML format. For a list of the file types that the DVA can convert, see *Oracle Outside In Technology Supported Formats* (http://www.oracle.com/technetwork/middleware/content-management/ds-oitfiles-133032.pdf).

Two GroupWise components rely on document conversion for their functionality:

- **Post Office Agent:** When GroupWise users access their mailboxes in any manner and use the Find feature to search for text, they expect to locate the text in attached documents as well as in email messages and other GroupWise items. For all GroupWise users, the DVA converts attached document files into HTML, so that attachments can be indexed by the POA.
- **GroupWise WebAccess:** When GroupWise users access their mailboxes through GroupWise WebAccess, they expect to view attached documents in their web browser, regardless of the file format of the attached file. For WebAccess users, the DVA converts attached document files into HTML so that the attachments can be viewed along with the email messages or other GroupWise items to which the documents are attached.

Because some document files contain unexpected data, they cannot be successfully converted into HTML format. The DVA isolates the document conversion task from other GroupWise activities. If the DVA encounters a problem converting a particular document file, the problem does not affect conversion of other document files, nor does it affect the user experience in GroupWise, except that the problem document cannot be viewed in WebAccess and cannot be located using the Find feature.

36 Scaling Your DVA Installation

If your GroupWise system is relatively small (one domain and a few post offices), a basic installation of one DVA along with each POA might meet your needs. However, if your GroupWise system is large or requires failover support, you can scale your DVA installation to better meet the reliability, performance, and availability needs of your GroupWise users.

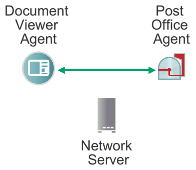
DVA Configurations

The following DVA configurations are possible, depending on the document conversion needs of your GroupWise users:

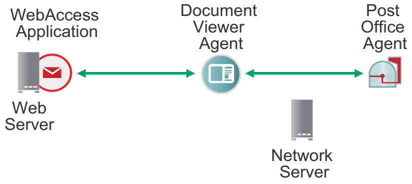
- "Basic DVA Installation" on page 363
- "Multiple DVAs for a Post Office" on page 364
- "Multiple DVAs for WebAccess" on page 364
- "Multiple Shared DVAs" on page 365

Basic DVA Installation

The DVA can be installed and configured along with the POA when you create a new post office. For background information, see "Adding a Post Office". You can also add the DVA to an existing post office where no DVA was originally set up.



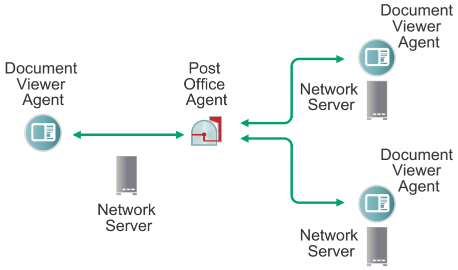
When you install WebAccess on a web server, you configure the WebAccess Application to communicate with any DVA in your GroupWise system.



Multiple DVAs for a Post Office

One DVA might provide sufficient indexing performance for the users in a post office, but you might want to protect against the downtime that would occur if the DVA became unavailable. Installing more than one DVA enables you to set up failover support to make document conversion and indexing more reliable.

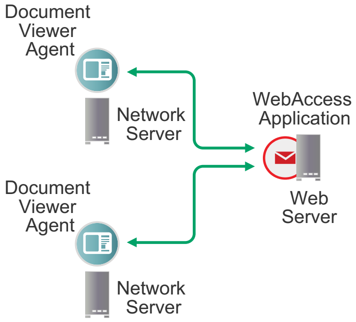
If you have a post office with a heavy load of attachment indexing, you can install and configure multiple DVAs to service the POA for that post office.



For more information about this configuration, see “Configuring the POA with Multiple DVAs for Indexing” on page 178.

Multiple DVAs for WebAccess

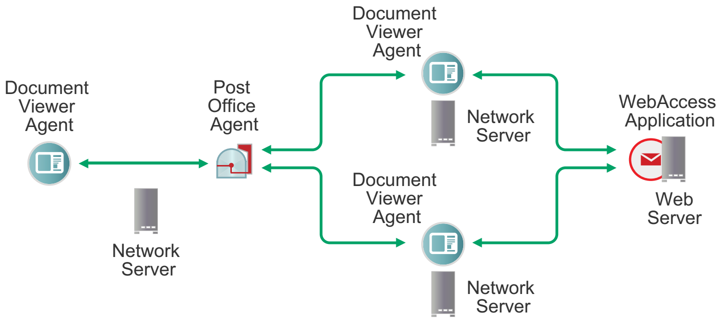
If GroupWise WebAccess users display a large number of attached documents, you can install and configure multiple DVAs to service the WebAccess Application so that attached documents can be displayed more promptly.



For more information about this configuration, see “Configuring WebAccess Application with Multiple DVAs for Attachment Viewing” on page 609.

Multiple Shared DVAs

When you install multiple DVAs, they can be accessed by both POAs and WebAccess Applications if that works well for your GroupWise system configuration.



Installing the DVA

The DVA can be installed and configured along with the POA when you create a new post office. For background information, see "Adding a Post Office". You can also add the DVA to an existing post office.

The DVA software is installed along with the GroupWise Server component. Then you use the GroupWise Administration Utility (GWAdminUtil) to configure the DVA as an agent service.

IMPORTANT: You can run only one DVA per server.

Linux: Installing and Starting the DVA

1 Ensure that the server where you install the DVA meets the system requirements listed in "Hardware and Operating System Requirements".

2 (Conditional) If you are setting up the DVA on a server where there is not a post office:

2a Install the GroupWise Server component.

Follow the instructions in Step 1 through Step 9 in "Linux: Installing the GroupWise Server Software" in the *GroupWise 18 Installation Guide* to install and start the GroupWise Admin Service, but do not start the Installation console. You do not need to create a post office in order to set up the DVA on the server.

2b Close GroupWise Installation Wizard.

2c Enter the following command to verify that the GroupWise Admin Service is running:

```
rcgrpwise status
```

2d Skip to Step 4.

3 (Conditional) If you are setting up the DVA on a server with a domain or post office, enter the following command to view the GroupWise agent services that are already set up on the server:

```
gwadminutil services --list
```

This list shows what is currently configured in the `gwha.conf` file. For background information about the `gwha.conf` file, see "Automatically Restarting the Linux GroupWise Agents with the GroupWise High Availability Service" in the *GroupWise 18 Installation Guide*.

4 Enter the following command to install the DVA as a service that can be managed by the GroupWise High Availability Service.

```
gwadminutil services -i -dva
```

5 Use the `list` command provided in Step 3 to see that the DVA is now configured as an agent service.

6 Enter the following command to check the statuses of all the GroupWise services on the server:

```
rcgrpwise status
```

Notice that the new DVA is not yet running.

7 Enter the following command to start the new DVA:

```
rcgrpwise start gwdva
```

8 Repeat the status command in Step 6 to verify that the new DVA is running.

You cannot start and stop the DVA in the GroupWise Admin console as you can the other GroupWise agents. You must mange the DVA on the command line.

9 Skip to "Setting Up the DVA" on page 367.

Windows: Installing and Starting a New DVA

1 Ensure that the server where you install the DVA meets the system requirements listed in "Hardware and Operating System Requirements".

2 (Conditional) If you want to set up a DVA on a server where there is not a post office:

2a Install the GroupWise Server component.

Follow the instructions in Step 1 through Step 9 in "Windows: Installing the GroupWise Server Software" in the *GroupWise 18 Installation Guide* to install, configure and start the GroupWise Admin Service, but do not start the Installation console. You do not need to create a post office in order to set up the DVA on the server.

2b Close GroupWise Installation Wizard.

2c Click **Control Panel > Administrative Tools > Services** to verify that the GroupWise Admin Service is running.

2d Skip to Step 4.

3 (Conditional) If you are setting up the DVA on a server with a domain or post office, click **Control Panel > Administrative Tools > Services** to view the GroupWise services that are already set up on the server.

4 At the Windows command prompt, enter the following command to set up the DVA as a Windows service.

```
gwsc -i -dva
```

5 Enter the following command to see that the DVA is now configured as an agent service.

```
gwsc --list
```

6 Refresh the list of Windows services to check the statuses of all the GroupWise services on the server.

Notice that the new DVA is not yet running.

7 Start the new DVA as you would start any other Window service.

   You cannot start and stop the DVA in the GroupWise Admin console as you can the other GroupWise agents. You must mange the DVA as a Windows service.

8 Continue with Setting Up the DVA.

Setting Up the DVA

After you install the DVA, you must make it available in your GroupWise system by creating an object for it and adding that DVA object to at least one POA.

Creating a DVA Object

After you install and start the DVA, you must create a DVA object, so that you can add the DVA to one or more POAs.

1 In the GroupWise Admin console, click **System > Document Viewer Agent**.

2 Click **New** to set up a new DVA.

3 In the **Name** field, specify a unique and descriptive name for the new DVA object.

   Do not use invalid characters.

4 In the **Address** field, specify the IP address or DNS hostname of the server where the DVA is running.

5 (Conditional) If the POA that the DVA will communicate with uses SSL, select **Enable SSL**.

   For more information, see "Securing the Post Office with SSL Connections to the POA" on page 152.

6 Click **OK** to create the new DVA object and add it to the list of DVAs in your GroupWise system.

7 Continue with Adding a DVA to a POA.

Adding a DVA to a POA

You can add a single DVA to one, two, or three POAs.

1 In the GroupWise Admin console, browse to and click the POA where you want to add the DVA.

2 Click the **Document Viewer Agent** tab.

3 Click **Add Document Viewer Agent**, then specify or select the DVA in the drop-down list.

4 Click **Save**, then click **Close**.

5 (Optional) Repeat Step 1 through Step 4 to add the DVA to additional POAs as needed.

The same result can be obtained by using POA startup switches. For more information, see "Configuring the POA with Multiple DVAs for Indexing" on page 178.

37 Configuring the DVA

The default configuration of the DVA is sufficient to provide basic document conversion functionality. The DVA is configured by editing its startup file (`startup.dva`).

Editing the startup.dva File

The location of the `startup.dva` file varies by platform:

Linux:	`/opt/novell/groupwise/agents/share`
Windows:	`c:\Program Files\Micro Focus\GroupWise Server\Agents`

You can use any ASCII text editor to edit the `startup.dva` file.

IMPORTANT: When you update the DVA software, a new `startup.dva` file is installed. The existing `startup.dva` file is retained as `startup.`*nnn*, where *nnn* increments each time you update the DVA software.

Setting the DVA Home Folder

The DVA home folder is named `gwdva`. The default location varies by platform:

Linux:	`/var/opt/novell/groupwise/gwdva`
Windows:	`c:\ProgramData\novell\groupwise\gwdva`

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

The DVA home folder has three subfolders (`quarantine`, `temp`, and `template`). If this folder consumes more disk space than you want consumed in the default location, you can move it to a different location on the local server or to a location on a remote server.

1 Open the `startup.dva` file in a text editor.

2 Search to find the following switch:

   `/home`

3 Remove the semicolon (;) to activate the setting.

4 Specify the full path name for the DVA home folder, for example:

Linux:	`/tmp/gwdva`

Windows:	`c:\temp\gwdva`
	`m:\gwsystem\gwdva`
	`\\gwserver5\c\gwsystem\gwdva`

On Windows, if you are running the DVA as a Windows service rather than as an application, the format you use for the path name influences the Windows user account that the DVA service can run under. If you specify a home folder on the local server or on a mapped drive, the DVA service can run under the local system account. If you specify a home folder as a UNC path to a remote server, the DVA service must run as a Windows user that has rights to access the remote home folder.

IMPORTANT: For simplicity of DVA administration, running the DVA as the Windows Administrator user is highly recommended.

---

5. (Optional) Use the --log switch to move the `log` subfolder out from under the DVA home folder.

   The `quarantine` folder cannot be moved.
6. Save the `startup.dva` file.
7. Skip to "Putting DVA Configuration Changes into Effect" on page 372.

Changing the DVA IP Address or Port Number

The DVA communicates with the other programs (the WebAccess Application, the POA, and the DVA console) by way of HTTP. By default, the DVA uses the first IP address it finds on the server and listens on port 8301.

1. Open the `startup.dva` file in a text editor.
2. Change the IP address:

   2a Search to find the following switch:

   ```
   /ip
   ```

   2b Remove the semicolon (;) to activate the setting.

   2c Specify the IP address that you want the DVA to use.
3. Change the port number:

   3a Search to find the following switch:

   ```
   /httpport
   ```

   3b Remove the semicolon (;) to activate the setting.

   3c Specify the port number that you want the DVA to use.

   Worker threads are assigned port numbers ascending above the main port number. For example, if you decide to use a main port number of 8500, the 5 default worker threads would be assigned ports 8501 through 8505. You must ensure that none of these incremental port numbers are already in use on the server, up to the largest possible number of DVA threads that could be started. For more information, see "Controlling Thread Usage" on page 377.
4. Save the `startup.dva` file.
5. Skip to "Putting DVA Configuration Changes into Effect" on page 372.

For information about how the DVA interacts with other programs, see:

- "Configuring WebAccess Application with Multiple DVAs for Attachment Viewing" on page 609
- "Configuring the POA with Multiple DVAs for Indexing" on page 178
- "Configuring the DVA Console" on page 373

Securing Document Conversion with SSL Connections

Secure Sockets Layer (SSL) ensures secure communication between the DVA and other programs (WebAccess Application, POA, and DVA console) by encrypting the complete communication flow between the programs. By default, SSL is not enabled for the DVA.

For background information about using SSL with GroupWise agents, see "Server Certificates and SSL Encryption" on page 695. The server where the DVA is installed must have a public certificate file and private key file before you can enable SSL for the DVA.

NOTE: When you enable SSL for the DVA, any POAs that it communicates with must also be enabled for SSL.

---

1 Open the `startup.dva` file in a text editor.
2 Search to find the following switch:

   `/httpssl`

3 Remove the semicolon (;) to activate the setting.
4 For subsequent switches:
   - **4a** Specify the full path name to the SSL public certificate file.

     The DVA requires that the certificate file be in PEM format.
   - **4b** Specify the full path name to the SSL private key file.
   - **4c** Specify the password for the private key file.
5 Save the `startup.dva` file.
6 Skip to "Putting DVA Configuration Changes into Effect" on page 372.

Enabling the DVA Document Quarantine

You can configure the DVA to quarantine document files that cannot be converted to HTML format for viewing in GroupWise WebAccess, so that they can be examined manually if necessary. You can control the maximum amount of disk space that the document quarantine is allowed to occupy. You can also control the maximum amount of time that document files remain in the quarantine.

1 Open the `startup.dva` file in a text editor.
2 Search to find the following switch:

   `/quarantine`

   With the quarantine activated, document files that fail HTML conversion are placed in the `quarantine` subfolder of the DVA home folder (gwdva).
3 Remove the semicolon (;) to activate the setting.
4 (Optional) As needed, increase or decrease the number of days that document files are held in quarantine.

   The default is 7 days.
5 (Optional) As needed, increase or decrease the amount of disk space that the quarantine is allowed to consume.

The default is 100 MB. Quarantined document files that exceed the maximum time limit are removed even if the maximum quarantine size has not been exceeded.

6 (Conditional) When you are finished examining the quarantined document files, set the maximum quarantine size to 0 (zero).

This disables the quarantine and deletes all the quarantined document files.

IMPORTANT: Quarantined document files are not encrypted, so you should disable the quarantine as soon as you are finished examining the quarantined files.

---

7 Save the `startup.dva` file.

8 Continue with Putting DVA Configuration Changes into Effect.

NOTE: If files passed to the DVA from the POA for HTML conversion in preparation for indexing fail in HTML conversion by the DVA, they are placed in the *`post_office`*`/oftemp/gwdca/problem` folder.

Putting DVA Configuration Changes into Effect

After you edit the `startup.dva` file, stop and then start the DVA to put the changes into effect.

- "Linux: Stopping and Starting the DVA" on page 372
- "Windows: Stopping and Starting the DVA" on page 372

Linux: Stopping and Starting the DVA

On Linux, use the following commands to stop and start the Linux DVA:

```
rcgrpwise stop gwdva
rcgrpwise start gwdva
```

Windows: Stopping and Starting the DVA

On Windows, stop and start the DVA as you would any other Windows GroupWise agent. For more information, see "Working with the GroupWise Agents" in the *GroupWise 18 Installation Guide*:

38 Monitoring the DVA

The DVA can be conveniently monitored in your web browser. You can also use log files to monitor the DVA.

Using the DVA Console

The web-based DVA console enables you to monitor the DVA from any location where you have access to a web browser and the Internet.

Configuring the DVA Console

1 Open the `startup.dva` file in a text editor.

2 To specify the user name for logging into the DVA console:

  2a Search to find the following switch:

  ```
  httpuser
  ```

  2b Remove the semicolon (;) to activate the setting.

  2c Specify a unique user name.

3 To specify the password for logging into the DVA console:

  3a Search to find the following switch:

  ```
  httppassword
  ```

  3b Remove the semicolon (;) to activate the setting.

  3c Specify the password for the console user.

  Unless you are using an SSL connection, do not use a LDAP directory user name and password because the information passes over the non-secure connection between your web browser and the DVA.

4 (Conditional) If the default DVA HTTP port of 8301 is already in use on the server:

  4a Search to find the following switch:

  ```
  httpport
  ```

  4b Remove the semicolon (;) to activate the setting.

  4c Specify a unique port number.

5 Save the `startup.dva` file.

6 Skip to "Putting DVA Configuration Changes into Effect" on page 372.

Viewing the DVA Console

1 In a web browser, enter the following URL:

  http://*server_address*:*port_number*

Replace *server_address* with the DVA server IP address or DNS hostname, and replace *port_number* with 8301 or whatever port number you have specified in the DVA startup file.

2 When prompted, enter the user name and password.

The DVA console is displayed.

Through the DVA console you can view the following information:

- **Status:** Displays how long the DVA has been up, the number of worker threads it has started, the peak number of threads that have been busy, statistics about the files the worker threads have processed, and the worker processes and the process IDs.
- **Configuration:** Displays the current settings of all the options that you can set in the DVA startup file (`startup.dva`). For more information, see Chapter 37, “Configuring the DVA,” on page 369.
- **Environment:** Displays server information such as name, operating system date, memory, processor utilization, and loaded modules.
- **Log Files:** Lets you view the contents of the DVA log files and the current log settings. For more information, see “Using DVA Log Files” on page 374.
- **Quarantine Files:** Indicates whether the document quarantine is enabled, and if so, what files have been quarantined. For more information, see “Enabling the DVA Document Quarantine” on page 371

You cannot use the console to change any DVA settings. Changes must be made through the DVA startup file (`startup.dva`).

Using DVA Log Files

Error messages and other information about DVA functioning are written to log files as well as displaying on the DVA server console (Windows only). Log files can provide a wealth of information for resolving problems with DVA functioning. Logging is enabled by default.

Locating DVA Log Files

The default location of the DVA log files varies by platform:

Linux:	`/var/log/novell/groupwise/gwdva`
Windows:	`c:\ProgramData\Micro Focus\GroupWise\gwdva\log`

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

You can change the location where the DVA creates its log files. For more information, see Configuring DVA Log Settings.

Configuring DVA Log Settings

1 Open the `startup.dva` file in a text editor.

2 Search to find the `Log Switches` section.

3 Adjust the following log settings as needed:

--loglevel: There are three log levels:

- **Normal (default)** Displays warnings and errors.
- **Verbose:** Displays the Normal log level information, plus information messages and user requests.
- **Diagnostic:** Displays all possible information. Use Diagnostic only if you are troubleshooting a problem with the DVA.

  The Verbose and Diagnostic log levels do not degrade DVA performance, but log files consume more disk space when Verbose or Diagnostic logging is in use.

--log: For the default location of DVA log files, see "Locating DVA Log Files" on page 374. Specify a different location for DVA log files as needed.

--logdays: Specify the number of days you want to retain the log files. The DVA retains log files for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 30 days.

--logmax: Specify the maximum amount of disk space you want to use for DVA log files. If the disk space limit is exceeded, the DVA deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 102400 KB (100 MB).

4. Save the `startup.dva` file.
5. Skip to "Putting DVA Configuration Changes into Effect" on page 372.

Viewing DVA Log Files

For the default location of the DVA log files, see "Locating DVA Log Files" on page 374

When logging is turned on, the DVA creates a new log file each day and each time it is restarted. Therefore, you find multiple log files in the log file folder. The first four characters represent the date (*`mmdd`*). The next three characters identify the agent (`dva`). A three-digit extension allows for multiple log files created on the same day. For example, a log file named `0518dva.001` indicates that it is a DVA log file created on May 18.

For convenience, you can view DVA log files in the DVA console.

Interpreting DVA Log File Information

On startup, the DVA records the DVA settings currently in effect. Thereafter, it logs events that take place, including errors.

Because the DVA consists of multiple threads, you might find it useful to retrieve the log file into an editor and sort it on the thread ID that follows the date and time information. Sorting groups all messages together for the same DVA thread. You can also use the search capability of the DVA web console to gather information about events that contain a specific string.

39 Optimizing the DVA

Controlling Thread Usage

By default, the DVA starts 5 worker threads for converting attached document files into HTML format. It adds threads as demand for document file conversion increases. By default, the DVA can start a maximum of 20 worker threads.

1 Open the `startup.dva` file in a text editor.

2 To set the initial number of worker threads to start:

   2a Search to find the following switch:

   ```
   /httpthread
   ```

   2b Remove the semicolon (;) to activate the setting.

   2c Specify the maximum number of worker threads that you want to the DVA to start automatically.

3 To set the maximum number of worker threads:

   3a Search to find the following switch:

   ```
   /httpmaxthread
   ```

   3b Skip to "Putting DVA Configuration Changes into Effect" on page 372.

   3c Specify the maximum number of worker threads that the DVA is allowed to start.

   You can increase the maximum number of worker threads to allow the DVA to use more server resources, or you can decrease the maximum number of worker threads to cause the DVA to use fewer server resources.

4 Save the `startup.dva` file.

5 Skip to "Putting DVA Configuration Changes into Effect" on page 372.

Controlling Maximum Document Conversion Size and Time Limits

If the DVA starts converting a very large document file, it can take a very long time to complete the conversion into HTML format. The maximum size limit for document files processed by the DVA is set by the program that sends the document files to the DVA for conversion. For more information, see:

- POA: "Controlling Maximum Document Conversion Size and Time" on page 179
- WebAccess: "Controlling Viewable Attachment Size" on page 617

40 Using DVA Startup Switches

The DVA is configured by editing its startup file (`startup.dva`). The default location for the startup file varies by platform.

Linux:	`/opt/novell/groupwise/agents/share`
Windows:	`c:\Program Files\Micro Focus\GroupWise Server\Agents`

When you update the agent software, the existing DVA startup file can be retained or overwritten as needed.

Linux:	When you use both the **Install** and **Configure** options in the Agent Installation program, the existing DVA startup file is backed up and then overwritten. When you use only the **Install** option, the existing DVA startup file is retained.
Windows:	When you select **Install the software files, but do not configure the agents** in the Agent Installation program, the existing DVA startup file is retained. When you do not select this option, the existing DVA startup file is backed up and then overwritten.

The table below summarizes DVA startup switches and how they correspond to configuration settings in the GroupWise Admin console.

Switch starts with: a b c d e f g h i j k l m n o p q r s t u v w x y z

Linux DVA	Windows DVA	GroupWise Admin console Settings
--cleanTmpInterval	N/A	N/A
--dhparm	/dhparm	N/A
--home	/home	N/A
--httpmaxthread	/httpmaxthread	N/A
--httppassword	/httppassword	N/A
--httpport	/httpport	N/A
--httpssl	/httpssl	N/A
--httpthread	/httpthread	N/A
--httpuser	/httpuser	N/A
--ip	/ip	N/A
--log	/log	N/A
--logdays	/logdays	N/A
--loglevel	/loglevel	N/A
--logmax	/logmax	N/A
--maxquarantineage	/maxquarantineage	N/A

Linux DVA	Windows DVA	GroupWise Admin console Settings
--maxquarantinesize	/maxquarantinesize	N/A
--maxtime	/maxtime	N/A
--PDFSizeThreshold	/PDFSizeThreshold	N/A
--PDFReturnNoImage	/PDFReturnNoImage	N/A
--quarantine	/quarantine	N/A
--sslcert	/sslcert	N/A
--sslciphersuite	/sslciphersuite	N/A
--sslkey	/sslkey	N/A
--sslkeypassword	/sslkeypassword	N/A
--ssloption	/ssloption	N/A

@startup_file_name

Specifies the location of the DVA startup file if you want to change it from the default location. The default location varies by platform:

Linux:	`/opt/novell/groupwise/agents/share`
Windows:	`c:\Program Files\Micro Focus\GroupWise Server\Agents`

--cleanTmpInterval

Specifies an interval when the /tmp directory is cleaned up on a Linux server. This switch only works on Linux. The default interval is 1440 minutes or once at day and it triggers at 1 AM.

	Linux DVA
Syntax:	--cleanTmpInterval *Time in Minutes*
Example:	--cleanTmpInterval 120

--dhparm

Specifies a Diffie-Hellman cipher parameters file used for SSL/TLS to replace the default parameters set by GroupWise. GroupWise uses default Diffie-Hellman parameters of 2048 bits to generate the DH key. A valid DH parameter is in PEM format.

	Linux DVA	Windows DVA
Syntax:	--dhparm *directory*/*pemfile*	/dhparm *directory*/*pemfile*
Example:	--dhparm /var/tmp/dh.pem	/dhparm C:\temp\dh.pem

--home

Specifies the path to the DVA home folder. The default location varies by platform:

Linux:	`/var/opt/novell/groupwise/gwdva`
Windows:	`c:\ProgramData\novell\groupwise\gwdva`

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

For background information, see "Setting the DVA Home Folder" on page 369.

	Linux DVA	Windows DVA
Syntax:	--home /*directory*	/home-[*drive*:]*dir* /home-*svr**sharename**dir*
Example:	--home /opt/novell/groupwise/gwdva	/home-\Program Files\Novel\GroupWise Server\gwdva /home-m:\temp\gwdva /home-\\\\server2\c\temp\gwdva

On Windows, if you are running the DVA as a Windows service rather than as an application, the format you use for the path name influences the Windows user account that the DVA service can run under. If you specify a home folder on the local server or on a mapped drive, the DVA service can run under the local system account. If you specify a home folder as a UNC path to a remote server, the DVA service must run as a Windows user that has rights to access the remote home folder.

--httpmaxthread

Specifies the maximum number of worker threads that the DVA can start. By default, the DVA creates new worker threads as needed to handle the current document conversion load, and the default is 20 threads. The maximum recommended setting is 30 as setting it higher can negatively impact the system. See "Controlling Thread Usage" on page 377.

	Linux DVA	Windows DVA
Syntax:	--httpmaxthread *number*	/httpmaxthread-*number*
Example:	--httpmaxthread 20	/httpmaxthread-20

See also --httpthread.

--httpport

Sets the HTTP port number used for the DVA to communicate with other programs (the POA, the WebAccess Application, and the DVA console). The default is 8301; the setting must be unique. See "Changing the DVA IP Address or Port Number" on page 370.

	Linux DVA	Windows DVA
Syntax:	--httpport *port_number*	/httpport-*port_number*
Example:	--httpport 8302	/httpport-8303

See also --httppassword, and --httpuser.

--httppassword

Specifies the password for the DVA to prompt for before allowing DVA status information to be displayed in your web browser in the DVA console. See "Configuring the DVA Console" on page 373.

	Linux DVA	Windows DVA
Syntax:	--httppassword *unique_password*	/httppassword-*unique_password*
Example:	--httppassword AgentWatch	/httppassword-AgentWatch

See also --httpport, and --httpuser.

--httpssl

Enables secure SSL connections between the DVA and other programs (the POA, the WebAccess Application, and your web browser for the DVA console). See "Securing Document Conversion with SSL Connections" on page 371.

	Linux DVA	Windows DVA
Syntax:	--httpssl	/httpssl

See also --sslcert, --sslkey, and --sslkeypassword.

--httpthread

Sets the default number of worker threads that the DVA starts. The default is 5 threads. As the document conversion load increases, the DVA starts additional worker threads until the number set by the --httpmaxthread startup switch is reached. See "Controlling Maximum Document Conversion Size and Time Limits" on page 377.

	Linux DVA	Windows DVA
Syntax:	--httpthread *threads*	/httpthread-*threads*

	Linux DVA	Windows DVA
Example:	--httpthread 10	/httpthread-15

See also --httpmaxthread.

--httpuser

Specifies the user name for the DVA to prompt for before allowing DVA status information to be displayed in a web browser at the DVA console. See "Configuring the DVA Console" on page 373.

	Linux DVA	Windows DVA
Syntax:	--httpuser *unique_name*	/httpuser-*unique_name*
Example:	--httpuser DVAWebCon	/httpuser-DVAWebCon

See also --httpport and --httppassword.

--ip

Specifies the IP address that the DVA listens on for HTTP requests from other programs (the POA, the WebAccess Application, and the DVA console). The default is the first IP address that the DVA finds on the server. See "Changing the DVA IP Address or Port Number" on page 370.

	Linux DVA	Windows DVA
Syntax:	--ip *IP_address*	/ip-*IP_address*
Example:	--ip 172.16.5.18	/ip-172.16.5.18

See also --httpport.

--log

Sets the folder where the DVA stores its log files. The default log file location varies by platform:

Linux:	`/var/log/novell/groupwise/gwdva`
Windows:	`c:\ProgramData\Micro Focus\GroupWise\gwdva\log`

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

For more information, see “Configuring DVA Log Settings” on page 374.

	Linux DVA	Windows DVA
Syntax:	--log /*dir*	/log-[*drive*:]*dir* /log-*svr**sharename**dir*
Example:	--log /gwsystem/logs	/log-\agt\log /log-m:\agt\log /log-\\\\server2\c\mail\agt\log

See also --loglevel, --logdays, and --logmax.

--logdays

Specifies how many days to keep DVA log files on disk. The default is 30 days. See “Configuring DVA Log Settings” on page 374.

	Linux DVA	Windows DVA
Syntax:	--logdays *days*	/logdays-*days*
Example:	--logdays 10	/logdays-14

See also --log, --loglevel, and --logmax.

--loglevel

Controls the amount of information logged by the DVA. Valid settings are Normal, Verbose, Diagnostic, and Off. The default is Normal. For more information, see “Configuring DVA Log Settings” on page 374.

	Linux DVA	Windows DVA
Syntax:	--loglevel *level*	/loglevel-*level*
Example:	--loglevel verbose	/loglevel-verbose

See also --log, --logdays, and --logmax.

--logmax

Sets the maximum amount of disk space for all DVA log files. When the specified disk space is consumed, the DVA deletes existing log files, starting with the oldest. The default is 102400 KB (100 MB). The maximum allowable setting is 102400000 (1 GB). See “Enabling the DVA Document Quarantine” on page 371.

	Linux DVA	Windows DVA
Syntax:	--logmax *kilobytes*	/logmax-*kilobytes*

	Linux DVA	Windows DVA
Example:	--logmax 130000	/logmax-1600

See also --log, --logdays, and --logmax.

--maxquarantineage

Specifies the maximum number of days that document files that fail in HTML conversion are retained in the quarantine. By default, the quarantine is disabled. See “Enabling the DVA Document Quarantine” on page 371

	Linux DVA	Windows DVA
Syntax:	--maxquarantineage *days*	/maxquarantineage-*days*
Example:	--maxquarantineage 15	/maxquarantineage-60

See also --quarantine and --maxquarantinesize.

--maxquarantinesize

Specifies in megabytes the maximum amount of disk space that the document quarantine can occupy. The default is 100 MB. To clear out the contents of the quarantine, set --maxquarantinesize to 0 (zero); this also disables the quarantine in the future. See “Enabling the DVA Document Quarantine” on page 371.

	Linux DVA	Windows DVA
Syntax:	--maxquarantinesize *megabytes*	/maxquarantinesize-*megabytes*
Example:	--maxquarantinesize 200	/maxquarantinesize-300

See also --quarantine and --maxquarantineage.

--maxtime

Specifies in seconds the maximum amount of time a DVA worker thread is allowed to work on a converting a single document file. The default is 120 seconds (2 minutes). Valid values range from10 seconds to 1200 seconds (20 minutes). See “Controlling Maximum Document Conversion Size and Time Limits” on page 377.

	Linux DVA	Windows DVA
Syntax:	--maxtime *seconds*	/maxtime-*seconds*
Example:	--maxtime 600	/maxtime-60

When the DVA provides HTML conversion for the POA, the setting of the DVA --maxtime switch interacts with the setting of the POA --dvamaxtime switch, which sets the amount of time that the POA waits for a response from the DVA.

--PDFSizeThreshold

Specifies the conversion size threshold for PDF documents requested from WebAccess. If a PDF has a lot of images, it can take a long time to convert. If this option is set, the DVA only returns the text from the PDF if the PDF exceedds the size threshold. The default is no limit. The value is set in MB.

	Linux DVA	Windows DVA
Syntax:	--PDFSizeThreshold *MB*	/PDFSizeThreshold -*MB*
Example:	--PDFSizeThreshold 500	/PDFSizeThreshold -500

--PDFReturnNoImage

Disables the DVA from returning any image during PDF document conversion. This overrides the --PDFSizeThreshold switch if it is set. This switch is either enabled or disabled. It is disabled by default.

--quarantine

Enables the document quarantine feature of the DVA, which is disabled by default. See "Enabling the DVA Document Quarantine" on page 371

	Linux DVA	Windows DVA
Syntax:	--quarantine	/quarantine

See also --maxquarantineage and --maxquarantinesize.

NOTE: If files passed to the DVA from the POA for HTML conversion in preparation for indexing fail in HTML conversion by the DVA, they are placed in the *post_office*/oftemp/gwdca/problem folder.

--sslcert

For secure SSL connections between the DVA and other programs (the WebAccess Application, the POA, and your web browser for the DVA console), specifies the full path name of the SSL certificate file. See "Securing Document Conversion with SSL Connections" on page 371.

	Linux DVA	Windows DVA
Syntax:	--sslcert /*folder*/*certificate_file*	/sslcert-[*drive*:]*dir**file* /sslcert-*svr**sharename**dir**file*
Example:	--sslcert /certs/gw.crt	/sslcert-\ssl\gw.crt /sslcert-m:\ssl\gw.crt /sslcert-\\\\server2\c\ssl\gw.crt

See also --httpssl, --sslkey, and --sslkeypassword.

--sslciphersuite

Sets the SSL cipher suites used by the Archive Agent, the Messaging Agent, and Messenger clients. The cipher list must be in OpenSSL format. For more information on OpenSSL format, see Cipher List Format (https://www.openssl.org/docs/apps/ciphers.html#CIPHER-LIST-FORMAT)

	Linux DVA	Windows DVA
Syntax:	--sslciphersuite *“setting”*	/sslciphersuite-*”setting*”
Example:	--sslciphersuite “HIGH:!AECDH:!EXP:@STRENGTH”	/sslciphersuite-”HIGH:!AECDH:!EXP:@STRENGTH”

--sslkey

Specifies the full path to the private file used to provide secure SSL communication between the DVA and other programs (the WebAccess Application, the POA, and the DVA console). See “Securing Document Conversion with SSL Connections” on page 371.

	Linux DVA	Windows DVA
Syntax:	--sslkey /*dir*/*file*	/sslkey-[*drive*:]*dir**file* /sslkey-*svr**sharename**dir**file*
Example:	--sslkey /certs/gw.key	/sslkey-\ssl\gw.key /sslkey-m:\ssl\gw.key /sslkey-\\\\server2\c\ssl\gw.key

See also --httpssl, --sslcert, and --sslkeypassword.

--sslkeypassword

Specifies the password used to encrypt the private SSL key file when it was created. See “Securing Document Conversion with SSL Connections” on page 371.

	Linux DVA	Windows DVA
Syntax:	--sslkeypassword *password*	/sslkeypassword-*password*
Example:	--sslkeypassword gwssl	/sslkeypassword-gwssl

See also --httpssl, --sslcert, and --sslkeypassword.

--ssloption

Specify a specific SSL protocol to disable. By specifying SSL_OP_NO_TLSv1, GroupWise will disable TLSv1 support. Specify additional options by adding the SSL key work separated by a comma.

	Linux DVA	Windows DVA
Syntax:	--ssloption *SSL_protocol*	/ssloption *SSL_protocol*
Example:	--ssloption SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1	/ssloption SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1

VIII Databases

41 Understanding GroupWise Databases

Your GroupWise system includes numerous databases where vital information is stored.

NOTE: The maximum size for all types of GroupWise databases is 4 GB. Domains, post offices, and mailboxes consist of multiple databases, so there are no physical size limits for domains, post offices, and mailboxes. However, there are feasibility limitations based on potentially time-consuming activities such as backup/restore procedures.

Domain Databases

The domain database (`wpdomain.db`) in each domain contains all administrative information for the domain, including:

- Address information about all GroupWise objects (such as users, resources, groups, and post offices) in the domain
- System configuration and linking information for the domain's MTA
- System configuration and linking information for the domain's GWIA (if there is one)
- Address and message routing information to other domains

The first domain you create is the primary domain. In the primary domain, the `wpdomain.db` file contains all administrative information for your entire GroupWise system (all domains, post offices, users, and so on). Because the `wpdomain.db` file in the primary domain is so crucial, you should back it up regularly and keep it secure. See "Backing Up a Domain" on page 421.

You can re-create your entire GroupWise system from the primary domain `wpdomain.db` file; however, if the primary domain `wpdomain.db` file becomes unusable, you can no longer make administrative updates to your GroupWise system.

Every domain you create after the primary domain is a secondary domain. The contents of secondary domains are automatically synchronized with the primary domain.

The database version for GroupWise 18 domain databases is 1420.

Post Office Databases

The post office database (`wphost.db`) in each post office contains all administrative information for the post office, including a copy of the GroupWise Address Book. This information is necessary for users to send messages to others in the GroupWise system.

The database version for GroupWise 18 post office databases is 1420.

User Databases

Each member of the post office has a personal database (`userxxx.db`) that represents the user's mailbox. The user database contains the following:

- Message header information
- Pointers to messages
- Personal groups
- Personal address books
- Rules

When a member of another post office shares a folder with one or more members of the local post office, a "prime user" database (`puxxxxx.db`) is created to store the shared information. The prime user is the owner of the shared information.

Local user databases and prime user databases are stored in the `ofuser` folder in the post office.

Because resources are addressable just like users, resources also have user databases.

Message Databases

Each member of the post office is assigned to a message database (`msgnnn.db`) where the body portions of messages are stored. Many users in a post office share a single message database. There can be as many as 255 message databases in the post office (numbered from 0 to 254). Message databases are stored in the `ofmsg` folder in the post office.

Outgoing messages from local senders are stored in the message database assigned to each sender. Incoming messages from users in other post offices are stored in the message database with the same name as the message database assigned to the sender in his or her own post office. In each case, only one copy of the message is stored in the post office, no matter how many members of the post office it is addressed to.

Library Databases

A library is a collection of documents and document properties stored in a database system that can be managed and searched. You do not need to set up libraries unless you are using GroupWise Document Management Services (DMS). See Part XIII, "Libraries and Documents," on page 511.

The databases for managing libraries are stored in the `gwdms` folder and its subfolders in the post office.

The `dmsh.db` file is a database shared by all libraries in the post office. It contains information about where each library in the post office is located.

Each library has its own subfolder in the `gwdms` folder. In each library folder, the `dmxxnn01-FF.db` files contain information specific to that library, such as document properties and what users have rights to access the library.

The actual documents in a library are not kept in the library databases. They are kept in a document storage area, which consists of a series of folders for storing documents. Documents are encrypted and stored in BLOBs (binary large objects) to make document management easier. A document, its versions, and related objects are stored together in the same BLOB.

A document storage area might be located in the post office itself, or in some other location where more storage space is available. If it is located in the post office, the document storage area can never be moved. Therefore, storing documents in the post office folder structure is not usually recommended. If it is stored outside the post office, a document storage area can be moved when additional disk space is required.

See Chapter 64, “Creating and Managing Libraries,” on page 515 and Chapter 66, “Creating and Managing Documents,” on page 527 for more information about Document Management Services.

Guardian Databases

The guardian database (`ngwguard.db`) serves as the master copy of the data dictionary information for the following subordinate databases in the post office:

- User databases (`userxxx.db`)
- Message databases (`msgnnn.db`)
- Prime user databases (`puxxxxx.db`)
- Library databases (`dmsh.db` and `dmxxnn01-FF.db`)

The guardian database is vital to GroupWise functioning. Therefore, the POA has an automated back-up and roll-forward process to protect it. The POA keeps a known good copy of the guardian database called `ngwguard.fbk`. Whenever it modifies the `ngwguard.db` file, the POA also records the transaction in the roll-forward transaction log called `ngwguard.rfl`. If the POA detects damage to the `ngwguard.db` file on startup or during a write transaction, it goes back to the `ngwguard.fbk` file (the “fall back” copy) and applies the transactions recorded in the `ngwguard.rfl` file to create a new, valid and up-to-date `ngwguard.db`.

In addition to the POA back-up and roll-forward process, you should still back up the `ngwguard.db`, `ngwguard.fbk`, and `ngwguard.rfl` files regularly to protect against media failure. Without a valid `ngwguard.db` file, you cannot access your email. With current `ngwguard.fbk` and `ngwguard.rfl` files, a valid `ngwguard.db` file can be rebuilt should the need arise.

The `ngwguard.dc` file is the structural template for building the guardian database and its subordinate databases. Also called a dictionary file, the `ngwguard.dc` file contains schema information, such as data types and record indexes. If this dictionary file is missing, no additional databases can be created in the post office.

42 Maintaining Domain and Post Office Databases

Occasionally, it is necessary to perform maintenance tasks on domain databases (`wpdomain.db`) or post office databases (`wphost.db`). The frequency depends on the reliability of your network and your own experience of how often problems are likely to occur.

NOTE: Unfortunately, damage to databases cannot be prevented. A power outage can occur in the middle of a write to a database. A hard drive can fail. However, the GroupWise tools for repairing damaged databases are very effective and should be able to resolve most damage to GroupWise databases.

To further protect your GroupWise system against loss of domain and post office information, see:

- Chapter 48, “Backing Up GroupWise Databases,” on page 421
- Chapter 49, “Restoring GroupWise Databases from Backup,” on page 423

To ensure that the same information exists in all domain and post office databases throughout your GroupWise system, see:

- “Replicating Secondary Domains, Post Offices, and Libraries” on page 412
- “Synchronizing the Primary Domain from a Secondary Domain” on page 412

Validating Domain or Post Office Databases

You can validate the data in the domain and post office databases at any time without interrupting normal GroupWise operation. The frequency can vary depending on the size of your system and the number of changes you make to users, resources, and groups.

1. In the GroupWise Admin console, connect to the domain where the database is located.
2. Browse to and click the name of the domain or post office where you want to validate the database.
3. From a domain, click **Maintenance**.

   or

   From a post office, click **Maintenance > Post Office Database**.
4. Select **Validate Database**, then click **Run**.

   You are notified if there are any physical problems, so you can then recover or rebuild the database. If the task takes a while to complete, see “Monitoring Background Administrative Tasks” on page 36.

   If the Validate process reveals problems with the database, see “Recovering Domain or Post Office Databases” on page 396 and “Rebuilding Domain or Post Office Databases” on page 398.

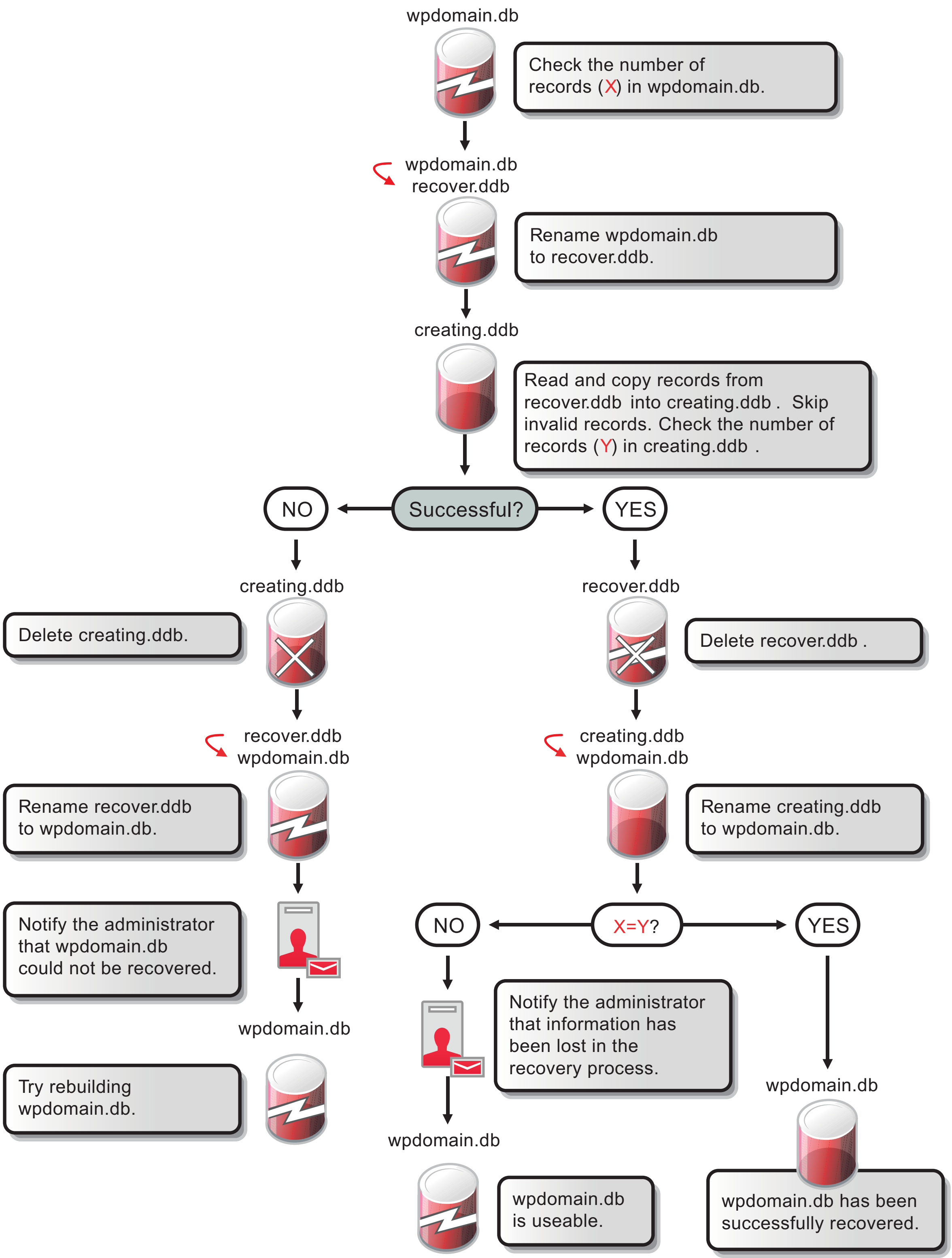
Recovering Domain or Post Office Databases

The database recover process corrects physical problems in the database structure, but does not update incorrect information contained in the database.

If you receive an administrative message informing you that an internal database error has occurred, or if you detect database damage and don't want to take users out of GroupWise, you can recover the database. If no errors are reported after the recover process, you do not need to take further action.

The recover process is run against a copy of the domain database (`wpdomain.db`) or post office database (`wphost.db`). Therefore, while the recover process is running, you can continue to access the database through the GroupWise Admin console and you do not need to stop the MTA or the POA.

As the copy of the database is created, the recover process skips invalid records. If the number of records in the original `wpdomain.db` file or `wphost.db` file is different from the number in the new, valid copy, GroupWise sends a notification message informing you that data has been lost. When the recover process is completed, the backup database is deleted.



For convenience, the agents are configured by default to automatically recover domain and post office databases whenever a physical problem is encountered. This setting can be changed on the Admin Task Status page in the POA console and the MTA console.

To recover a specific database in the GroupWise Admin console:

1. Ensure that you have sufficient disk space for the copy of the database that is created during recovery.
2. In the GroupWise Admin console, connect to the domain where the database is located.
3. Browse to and click name of the domain or post office where you want to recover the database.
4. From a domain, click **Maintenance**.

   or

   From a post office, click **Maintenance > Post Office Database**.
5. Select **Recover Database**, then click **Run**.

   You are notified if there are any physical problems, so you can then rebuild the database. If the task takes a while to complete, see "Monitoring Background Administrative Tasks" on page 36.
6. Click **Close** to return to the main Admin console window.

If recovery is successful, the backup database is deleted, and the new domain database is renamed to `wpdomain.db`, or the new post office database is renamed to `wphost.db`.

If recovery fails for any reason, the backup database is copied back to `wpdomain.db` or `wphost.db`. If any data was lost, you are notified by an administrative message.

You have several options for retrieving lost data from other sources:

- If data has been lost from the primary domain, you can synchronize it with a secondary domain that is known to contain current information. See "Synchronizing the Primary Domain from a Secondary Domain" on page 412.
- If data has been lost from a secondary domain, you can replicate the information from the primary domain. See "Replicating Secondary Domains, Post Offices, and Libraries" on page 412.
- You can also rebuild the database at a later time when you have exclusive access to the database where the data has been lost. See "Rebuilding Domain or Post Office Databases" on page 398.

Rebuilding Domain or Post Office Databases

In addition to correcting the physical problems resolved by the database recover process, the rebuild process updates object information in a domain database (`wpdomain.db`) or post office database (`wphost.db`). However, the process requires that no GroupWise agents (MTA or POA) have access to the database during the rebuild process.

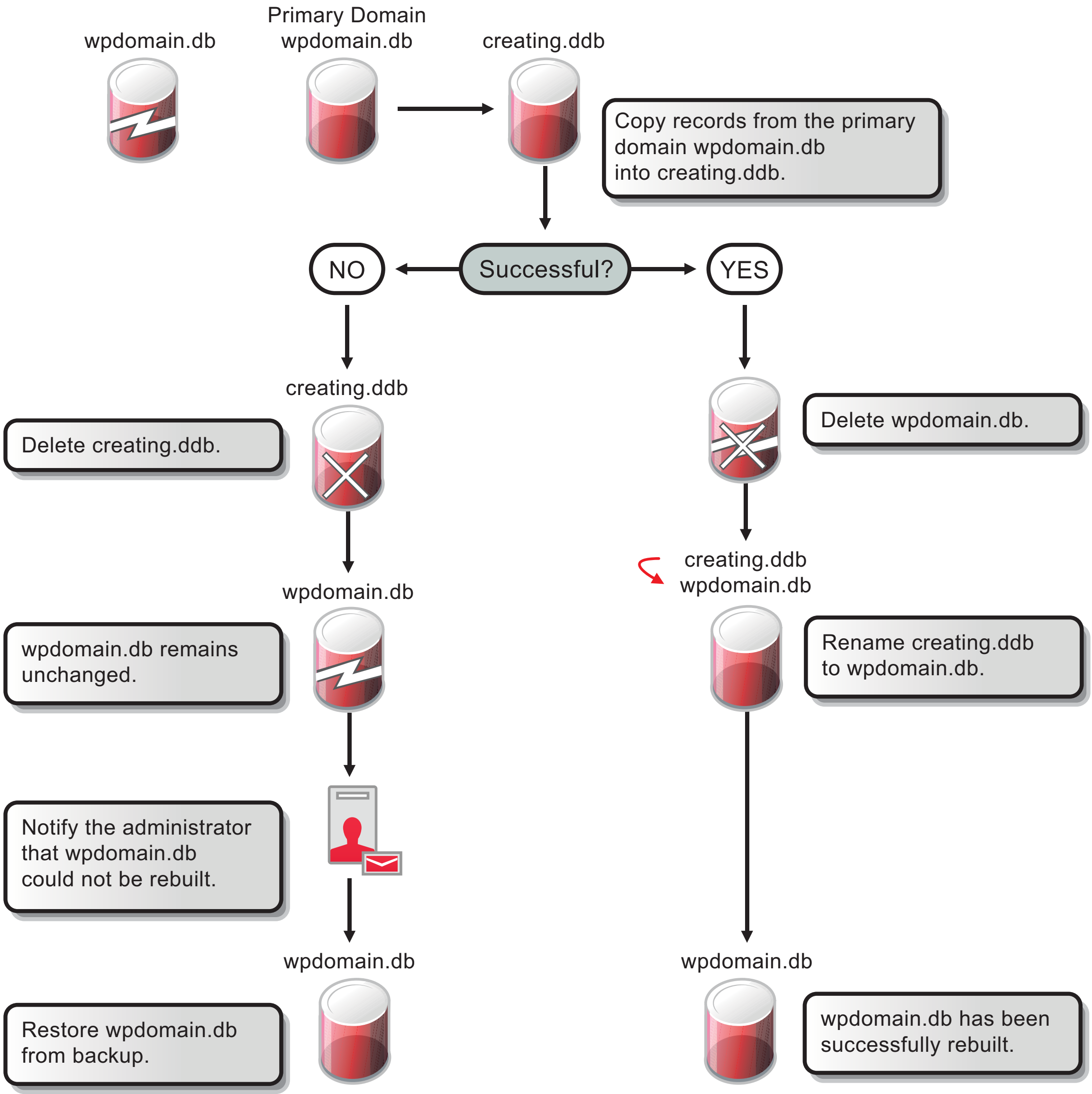
You should rebuild a domain or post office database if you encounter any of the following conditions:

- Objects are not being replicated between domains.
- The agent that writes to the database went down unexpectedly.
- The server where the database resides went down unexpectedly.
- You receive a notification message informing you that an internal database error has occurred or there is database damage and you think there might be data loss.
- You ran the recover database process and received a notification of data loss.

When you rebuild a secondary domain database, information is retrieved from the primary domain. When you rebuild a post office database, information is retrieved from the owning domain.

IMPORTANT: If you need to rebuild a secondary domain database that is a version previous to GroupWise 18, use gwadminutil to rebuild the database.

During the rebuild process, a backup of the domain or post office database is created as well as a new `wpdomain.db` or `wphost.db`. The records from the primary domain database are copied into the new `wpdomain.db`. There should not be any data loss. When the rebuild process is complete, the temporary database and the backup database are deleted.



To rebuild a database:

1 Ensure that you have sufficient disk space for the copy of the database that is created during the rebuild process.

2 In the GroupWise Admin console:

2a (Conditional) If you are rebuilding a secondary domain database, connect to the primary domain.

NOTE: If you need to rebuild the primary domain database, you must use the GroupWise Administration Utility (gwadminutil). For instructions, see Rebuilding a Domain or Post Office Database in the *GroupWise 18 Utilities Reference*.

or

2b (Conditional) If you are rebuilding a post office database, connect to the domain that owns the post office.

3 Browse to and click the name of the domain or post office where you want to rebuild the database.

4 From a domain, click **Maintenance**.

or

From a post office, click **Maintenance > Post Office Database**.

5 Select **Rebuild Database**.

6 Stop the agent that accesses the database.

If you are rebuilding a post office database, stopping the POA prevents users from accessing their mailboxes while the rebuild is in progress.

7 Click **Run**.

If the task takes a while to complete, see "Monitoring Background Administrative Tasks" on page 36.

8 Click **Close** to return to the main Admin console window.

9 Restart the agent that accesses the rebuilt database.

Replacing the Primary Domain Database with a Secondary Domain Database

If the primary domain database (`wpdomain.db`) has become extremely damaged and you do not have a current backup of it, you can replace the primary domain database with the contents of a secondary domain database.

1 In the GroupWise Admin console, connect to the secondary domain.

2 Browse to and click the name of the primary domain.

3 Click **Maintenance**, then select **Replace Primary with Secondary**.

4 Stop the MTA and the GWIA, then click **Run**.

A dialog box displays progress on the task.

5 Click **Close** to return to the main Admin console window.

6 (Optional) To manage tasks in the **Action Status Information** list, click the task number in the upper right corner of the main Admin console window to display the Notifications window.

7 Restart the MTA and the GWIA.

Rebuilding Database Indexes

Each domain database (`wpdomain.db`) and post office database (`wphost.db`) contains three indexes that are used to determine the order of the Address Book: the system index, the domain index, and the post office index. When you display the GroupWise Address Book, the system index is used. When you display a domain-level Address Book, the domain index is used, and when you display the Address Book for a post office, the post office index is used.

The GroupWise client uses the post office database to list users. If you are in the GroupWise client and the indexes for listing system, domain, and post office users are different than the domain database indexes, you should rebuild the post office database indexes.

To rebuild a database index:

1. In the GroupWise Admin console, connect to the domain that owns the database.
2. Browse to and click the name of the domain or post office where you want to rebuild the database index.
3. From a domain, click **Maintenance**.

   or

   From a post office, click **Maintenance > Post Office Database**.
4. Select **Rebuild Indexes**.
5. Click **Run**.

   If the task takes a while to complete, see "Monitoring Background Administrative Tasks" on page 36.
6. Click **Close** to return to the main Admin console window.

43 Maintaining User/Resource and Message Databases

It is sometimes necessary to perform maintenance tasks on user and resource databases (`userxxx.db`) and message databases (`msgnnn.db`). The frequency depends on the reliability of your network and your own experience of how often problems are likely to occur. The following sections help you maintain the integrity of your user and message databases.

NOTE: Unfortunately, damage to databases cannot be prevented. A power outage can occur in the middle of a write to a database. A hard drive can fail. However, the GroupWise tools for repairing damaged databases are very effective and should be able to resolve most damage to GroupWise databases.

To further protect your GroupWise users against loss of mailbox contents, see Chapter 48, “Backing Up GroupWise Databases,” on page 421 and Chapter 49, “Restoring GroupWise Databases from Backup,” on page 423.

To ensure that the same information exists for users and messages throughout your GroupWise system, see “Replicating Users, Resources, and Groups” on page 411.

Recovering User/Resource and Message Databases

By default, the POA automatically recovers any user/resource or message database where invalid structure or information is detected. Whenever a database is recovered, the domain’s notification user receives a message in GroupWise. For more information, see “Receiving Notifications of Agent Problems” on page 242.

By default, the POA can use up to 4 maintenance handler threads for database recovery. You can changed the maximum number of threads as needed.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Maintenance** tab.
3. Locate the **Automatic Database Recovery** section and adjust the number of maintenance handler threads, as needed.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Analyzing and Fixing User/Resource and Message Databases

The Analyze/Fix option of Mailbox/Library Maintenance looks for problems and errors in user and resource databases (`userxxx.db`) and/or message databases (`msgnnn.db`) and then fixes them if you select the **Fix Problems** option. You can analyze databases individually or you can analyze all user, resource, and/or message databases in one or more post offices.

To analyze and repair user, resource, and/or message databases:

1 In the GroupWise Admin console, browse to and click the name of the user or resource whose message databases you would like to analyze/fix.

   or

   Browse to and select one or more Post Office objects to select all user and/or message databases in the post office.

2 Click **Maintenance > Mailbox/Library Maintenance**.

3 From the **Actions** drop-down menu, select **Analyze/Fix Databases**.

4 Select from the following options:

   Structure: When a user experiences a problem that is related to the user, message, or library databases, you should perform a structure check. The structure check verifies the integrity of the databases and reports the amount of space that could be recovered. If there is a structural problem, the databases are rebuilt with free space reclaimed.

   Index Check: If you select **Structure**, you can also select **Index Check**. You should run an index check if a user tries to open a message and gets a read error, or when sent items that show a delivered status in the Properties window do not appear in the recipient's mailbox. An index check can be time-consuming.

   Contents: The user databases (located in the `ofuser` folder) do not contain user messages. Messages are contained in the message databases under the `ofmsg` folder. However, the message databases do not contain the message attachments; these are located in the `offiles` folder. A contents check analyzes references to other items. For example, in the user database, Mailbox/Library Maintenance verifies that any referenced messages actually exist in the message database. In the message database, it verifies that any attachments that are referenced actually exist in the attachment folders. A contents check also restores system folders (Mailbox, Sent Items, Calendar, Cabinet, and Trash to their default locations if any of them have been moved into a subfolder.

   Collect Statistics: If you selected **Contents**, the **Collect Statistics** option is available to collect and display statistics about the post office, such as the number of messages and appointments in the post office and the average number per user. In addition, you can display any user mailboxes that have more than a specified number of items. This can help determine if some users are using an excessive amount of disk space. If this is a problem, you might want to encourage users to delete unneeded items or to use the Archive feature in the GroupWise client to store messages on their local drives. You can also limit the amount of disk space each user can have. See "Managing Disk Space Usage in the Post Office" on page 121.

   Attachment File Check: Files that are attached to messages are stored under the `offiles` subfolder in the post office. When Mailbox/Library Maintenance performs an attachment file check, it reads each attachment file, verifying the file structure. If you skip the attachment file check, Mailbox/Library Maintenance verifies that the attachment file exists but it does not process the file in any way.

   Fix Problems: This option tells Mailbox/Library Maintenance to fix any problems it finds. Otherwise, Mailbox/Library Maintenance just reports the problems.

   Update User Disk Space Totals: Recalculates the total disk space a GroupWise user is using by reading the selected user mailboxes and updating the poll record used for disk space management. Because disk space is user-specific, the program calculates the amount of disk space in use by the user in the user databases, in any of the message databases, and in the attachment folder. Disk space limitations do not take into account the disk space used in document libraries. This option is usually run if the user totals are not being reflected correctly.

5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

“Databases” on page 436
“Logging” on page 437
“Results” on page 437
“Misc” on page 437
“Exclude” on page 437

Selected options can be saved for repeated use. See “Saving Mailbox/Library Maintenance Options” on page 437.

6 Click **OK** to perform the Analyze/Fix operation.

TIP: You can also perform this task for more than one user or resource at a time by using the **Maintenance > Mailbox/Library Maintenance** dialog on the Post Office where the users or resources are located, then selecting **Maintenance on User/Resources on this Post Office**.

Analyze/Fix can also be run using the stand-alone GroupWise Check program. See “GroupWise Check” on page 433. It can also be scheduled to run on a regular basis by properly configuring the POA. See “Scheduling Database Maintenance” on page 154.

Performing a Structural Rebuild of a User/Resource Database

The Structural Rebuild option of Mailbox/Library Maintenance rebuilds the structure of a user or resource database (`user`*`xxx`*`.db`) and reclaims any free space. It does not re-create the contents of the database. If you need to recover database contents as well as structure, see “Re-creating a User/ Resource Database” on page 406.

To rebuild a user database:

1 In the GroupWise Admin console, browse to and click the name of the user or resource whose database needs to be rebuilt.

2 Click **Maintenance > Mailbox/Library Maintenance**.

3 From the **Action**s drop-down list, select **Structural Rebuild**.

4 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

“Databases” on page 436
“Logging” on page 437
“Results” on page 437
“Misc” on page 437

Selected options can be saved for repeated use. See “Saving Mailbox/Library Maintenance Options” on page 437.

5 Click **Run** to perform a structural rebuild of the user database.

TIP: You can also perform this task for more than one user or resource at a time by using the **Maintenance > Mailbox/Library Maintenance** dialog on the Post Office where the users or resources are located, then selecting **Maintenance on User/Resources on this Post Office**.

Re-creating a User/Resource Database

The **Re-create User Database** option of Mailbox/Library Maintenance rebuilds a user or resource database (`user`*`xxx`*`.db`) and recovers any information it can. Some information is lost, such as the folder assignments.

You should never need to select this option for regular database maintenance. It is designed for severe problems, such as replacing a user database that has been accidentally deleted and for which you have no backup copy. A substantial amount of information is lost in the re-creation process. For a list of the data, see "User Databases" on page 136.

Because folder assignments are lost, all items are placed into the Cabinet folder. The user must then reorganize all the items in his or her mailbox. Using filters and searching can facilitate this process, but it is not a desirable experience. It is, however, preferable to losing everything.

To re-create a user database:

1. In the GroupWise Admin console, browse to and click the name of the user or resource that need the user database re-created.
2. Click **Maintenance > Mailbox/Library Maintenance.**
3. From the **Actions** drop-down list, select **Recreate User Database.**
4. Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

   "Databases" on page 436
   "Logging" on page 437
   "Results" on page 437
   "Misc" on page 437

   Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 437.
5. Click **OK** to re-create the user database.

TIP: You can also perform this task for more than one user or resource at a time by using the **Maintenance > Mailbox/Library Maintenance** dialog on the Post Office where the users or resources are located, then selecting **Maintenance on User/Resources on this Post Office**.

---

44 Maintaining Library Databases and Documents

GroupWise Document Management Services (DMS) uses libraries as repositories for documents. For a review of library database structure, see "Library Databases" on page 392.

- "Analyzing and Fixing Databases for Libraries and Documents" on page 407
- "Analyzing and Fixing Library and Document Information" on page 408

NOTE: Unfortunately, damage to databases cannot be prevented. A power outage can occur in the middle of a write to a database. A hard drive can fail. However, the GroupWise tools for repairing damaged databases are very effective and should be able to resolve most damage to GroupWise databases.

Analyzing and Fixing Databases for Libraries and Documents

For libraries, the **Analyze/Fix Databases** option of Mailbox/Library Maintenance looks for problems and errors in library and document databases and then fixes them if you select the **Fix Problems** option.

1 In the GroupWise Admin console, browse to and click the name of the name of the library that you want to analyze/fix.

2 Click **Maintenance > Mailbox/Library Maintenance.**

3 From the **Action** drop-down menu, select **Analyze/Fix Databases**.

4 Select from the following options:

Structure: When a user experiences a problem that is related to the library databases, you should perform a structure check. The structure check verifies the integrity of the databases and reports the amount of space that could be recovered. If there is a structural problem, the databases are rebuilt with free space reclaimed.

Index Check: If you select **Structure**, you can also select **Index Check**. An index check can be time-consuming.

Contents: The library database (located in the gwdms folder of the post office) does not contain documents. Documents are stored in the `lib0000-FF` folders. A contents check analyzes references from libraries to documents.

Collect Statistics: If you selected **Contents**, the **Collect Statistics** option is available to collect and display statistics about the library, such as the number and size of documents.

Attachment File Check: Files that are attached to messages are stored under the `offiles` subfolder in the post office. When Mailbox/Library Maintenance performs an attachment file check, it reads each attachment file, verifying the file structure. If you skip the attachment file check, Mailbox/Library Maintenance verifies that the attachment file exists but it does not process the file in any way.

Fix Problems: This option tells Mailbox/Library Maintenance to fix any problems it finds. Otherwise, Mailbox/Library Maintenance just reports the problems.

5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

"Databases" on page 436
"Logging" on page 437
"Results" on page 437
"Misc" on page 437

Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 437.

6 Click **OK** to perform the Analyze/Fix Databases operation on the library.

TIP: You can also perform this task for more than one library object at a time by using the **Maintenance > Mailbox/Library Maintenance** dialog on the Post Office where the library objects are located, then selecting **Maintenance on Libraries on this Post Office**.

Analyze/Fix Databases can also be run using the stand-alone GroupWise Check program. See "GroupWise Check" on page 433. It can also be scheduled to run on a regular basis by properly configuring the POA. See "Scheduling Database Maintenance" on page 154.

Analyzing and Fixing Library and Document Information

The Analyze/Fix Library option of Mailbox/Library Maintenance performs more library-specific functions than Analyze/Fix Databases. For all options except Verify Library, all documents in each of the selected library databases are checked. This can be a time-consuming process. Therefore, if you intend to select more than one of the Analyze/Fix Library options, you can save time by selecting each of them before you run them. This causes all selected options to be run against each document, which is faster than running each option individually against all documents.

To validate library databases:

1 In the GroupWise Admin console, browse to and click the name of the name of the library that you want to validate.

2 Click **Maintenance > Mailbox/Library Maintenance.**

3 From the **Action** drop-down menu, select **Analyze/Fix Library**.

4 Select from the following options:

Verify Library: This is a post office-level check. It verifies that all libraries are on the libraries list. It also checks the schema and guarantees its integrity. If there is a problem with the schema, it resets to a default schema to reclaim any missing items. For example, if you deleted the Document Type property, you could recover it using this option.

Fix Document/Version/Element: This performs an integrity check to verify the following:

- Each document has one or more versions linked to it.
- Each version has one or more elements linked to it.
- All versions are linked to a document.
- All elements are linked to a version.

If there are any missing links, the missing documents or versions are created from the information contained in the existing version or element for which the link is missing. For example, if a version is found that shows no link to a document, a document is created from the

information contained in the version and the link is reestablished. Of course, any information in the lost document that might have been newer than the information contained in the old version is lost.

Verify Document Files: This determines if the BLOB exists for a document and the document is accessible. If not, an error is logged for that document. The log message does not indicate why a file is missing or inaccessible. You can recover a file by restoring it from backup.

Possible errors that would be logged include:

- If the file system on the network becomes corrupted, this tells you which documents cannot be opened or which BLOB files are missing.
- If a file was marked by someone as Read Only or Hidden, this option logs an error indicating that the file is inaccessible.

Validate All Document Security: This option validates document security for the Author, Creator and Security (document sharing) fields. The validation replaces the results of selecting the **Validate Author/Creator Security** option, and is more thorough. Therefore, you only need to select one option or the other.

Synchronize User Name: The **Author** and **Creator** fields display users' full names, not unique IDs. If a user's name is changed, such as for marriage, this option verifies that the user's name on document and version records is the same as the user's current display name. In other words, the **Author** and **Creator** fields in documents and versions are updated to the user's newer name.

Remove Deleted Storage Areas: When you delete a document storage area on the Library **Storage Areas** tab, the document storage area and the documents stored there remain on the system. Deleting the storage area from the library only means that new documents are not stored there. The documents there continue to be available to users.

If you want to also remove the document storage area from the system, you have two options: delete the storage area and its documents, or first move the documents and then delete the storage area. The first option is not advisable, but exists so that if you have moved all of the documents that can be moved, but some corrupted documents are left behind, you can force the document storage area to be deleted.

You should normally select **Move Documents First** so that users continue to have access to those documents from a different document storage area. With this option, all BLOBs in the library are checked to see which documents are in the area being deleted.

Reassign Orphaned Documents: Documents can occasionally become orphaned (unattached to a user). For example, this can happen when a user leaves your organization and the user object is removed. All documents belonging to that user are no longer available in GroupWise searches and cannot be accessed by anyone (document security is controlled by the user listed in the **Author** and **Creator** fields). This option lets you reassign these documents to another user. You must select a new author from the browser menu after checking this option. The new author you designate has access to all orphaned documents in this library.

Reset Word Lists: Documents stored in a library are indexed and inserted into a generated word list. This allows users to search for a document by keywords as well as any word contained within a document. The document library word list might become outdated and if this occurs, the word list must be regenerated. This option allows the program to regenerate the document library word list the next time an index operation is performed.

5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

"Databases" on page 436
"Logging" on page 437
"Results" on page 437

“Misc” on page 437

Selected options can be saved for repeated use. See “Saving Mailbox/Library Maintenance Options” on page 437.

6 Click **OK** to perform the Analyze/Fix Library operation.

TIP: You can also perform this task for more than one library object at a time by using the **Maintenance > Mailbox/Library Maintenance** dialog on the Post Office where the library objects are located, then selecting **Maintenance on Libraries on this Post Office**.

Analyze/Fix Library can also be run using the stand-alone GroupWise Check program. See “GroupWise Check” on page 433. It can also be scheduled to run on a regular basis by properly configuring the POA. See “Scheduling Database Maintenance” on page 154.

45 Replicating Database Information

In general, replication of object information throughout your GroupWise system occurs automatically. Whenever you add, delete, or modify a GroupWise object, the information is automatically replicated to all appropriate databases. Ideally, each domain database (`wpdomain.db`) in your system contains original records for all objects it owns and accurately replicated records for all objects owned by other domains. However, because unavoidable events such as power outages and hardware problems can disrupt network connectivity, information in various databases might become inconsistent.

If you think you have a replication problem, especially soon after adding, deleting, or modifying objects, it is wise to check Pending Operations to ensure that your changes have been processed. See "Pending Operations" on page 54. When waiting for replication to take place, patience is a virtue.

When information differs between the original record and a replicated record, the original record is considered correct. If you perform replication from the owning domain, the owning domain notifies the primary domain of the correct information, then the primary domain broadcasts the correct information to all secondary domains. Therefore, the best place to perform replication is from the domain that owns the object whose information as become inconsistent. The next best place to perform replication is from the primary domain, because the primary domain sends a request to the owning domain for the correct information, then broadcasts the correct information to all secondary domains.

Replicating Users, Resources, and Groups

Most often, you will notice a replication problem when a user has trouble sending a message. Symptoms include:

- The sender receives a "user is undeliverable" message.
- A new user, resource, or group does not appear in the Address Book in some or all post offices.
- User, resource, or group information is incorrect in the Address Book but correct in the GroupWise Admin console.
- A user, resource, or group is listed in the Address Book as belonging to one post office but actually belongs to another.

To replicate User, Resource, and Group objects:

1. In the GroupWise Admin console, browse to and click the name of the user, resource, or group.
2. Click **More > Replicate**.

   The task to replicate the object is passed to the GroupWise Admin Service for processing.

If many User, Resource, and Group objects are being replicated, you can check progress by viewing pending operations. See "Pending Operations" on page 54.

After replication is complete, you can verify that it was successful by checking the replicated objects in Address Books and several post offices in your GroupWise system.

If there are indications that a large number of User or Resource objects need to be synchronized, rebuilding the post office database (`wphost.db`) can be preferable to synchronizing individual objects. However, this process requires exclusive access to the post office database. See "Rebuilding Domain or Post Office Databases" on page 398.

Replicating Secondary Domains, Post Offices, and Libraries

If information for a particular secondary domain, post office, or library does not display the same throughout your GroupWise system, you can replicate the object.

1. In the GroupWise Admin console, browse to and click the name of the domain, post office, or library.
2. (Conditional) For a secondary domain, if there is any doubt about the correctness of that secondary domain's information as stored in the primary domain database, synchronize the primary domain with the secondary domain before proceeding.

   See "Synchronizing the Primary Domain from a Secondary Domain" on page 412.
3. Click **More > Replicate**.

   The task to replicate the object is passed to the GroupWise Admin Service for processing.

After replication is complete, you can verify that it was successful by checking the domain, post office, or library information when connected to different domains in your GroupWise system.

See also the following related topics:

- "Rebuilding Domain or Post Office Databases" on page 398
- "Analyzing and Fixing Library and Document Information" on page 408

Synchronizing the Primary Domain from a Secondary Domain

Information about a secondary domain that is stored in the secondary domain database is considered more current and correct than information about that secondary domain that is stored in the primary domain database. If the primary domain database contains out-of-date information, you can synchronize the primary domain from the secondary domain.

When you synchronize the primary domain database from a secondary domain database, any records the secondary domain owns, such as post offices or users added to the secondary domain, are replicated from the secondary domain database to the primary domain database.

You must use the GroupWise Administration Utility (GWAdminUtil) to synchronize the primary domain from a secondary domain because direct file access to both databases is required.

To synchronize the primary domain from a secondary domain:

1. From the primary domain server, establish direct file access to the secondary domain server.

   On Linux, mount the file system on the secondary domain server to the primary domain server. On Windows, map a drive from the primary domain server to the secondary domain server.
2. Use the following command to synchronize the primary domain from the secondary domain:

   ```
   gwadminutil sync --primary /path_to_primary_domain_database
                    --domain /path_to_secondary_domain_database
   ```
3. To ensure that the primary domain database is totally up-to-date, repeat Step 1 and Step 2 for each secondary domain in your system.

46 Managing Database Disk Space

One of the most common maintenance issues in a growing system is running out of disk space. In addition to sending messages, users tend to use GroupWise for all sorts of communication, such as transferring large files. Library documents created with Document Management Services (DMS) can use huge amounts of disk space. Archived library documents can also quickly use up disk space assigned to the post office, where space is usually limited.

You should let your users know about the archive and auto-delete features of GroupWise mail, or set Client Options in the GroupWise Admin console to automatically archive or delete. See Chapter 69, “Setting Defaults for the GroupWise Client Options,” on page 545.

See also “Managing Disk Space Usage in the Post Office” on page 121.

Gathering Mailbox Statistics

If you have some users who don’t like to throw anything away, you might want to monitor the size of their mailboxes and, where appropriate, suggest voluntary cleanup. You can assess email retention by the number of messages, age of messages, or size of user databases.

The Mailbox Statistics option in Mailbox/Library Maintenance collects and displays statistics about the post office, such as the number of messages and appointments in the post office and the average number per user. It is valid only for user databases. In addition, you can display any user mailboxes that have more than a specified number of items. This can help determine which users might be using an excessive amount of file server disk space.

To gather mailbox statistics:

1 In the GroupWise Admin console, browse to and click the name of the user, resource, or post office.

2 For a user or resource, click **Maintenance**.

   or

   For a post office, click **Maintenance > Mailbox/Library Maintenance**.

3 From the **Action**s drop-down menu, select **Mailbox Statistics**.

4 Select **Mailbox Statistics**.

   Mailbox Statistics: Specify a maximum number of items to see a report showing each user whose mailbox has more items in it than the number you specify.

   or

   Select **Expire Statistics**.

   Expire Statistics: Select one of the following:

   - **Items Older Than:** Shows how many items are older than the number of days you specify.
   - **Downloaded Items Older Than:** Shows how many items have been downloaded to users’ GroupWise Caching or Remote mailboxes that are older than the number of days you specify. This does not include items that have been downloaded to non-GroupWise mailboxes (for example, POP and IMAP accounts).
   - **Items Larger Than:** Shows how many items are larger than the size you specify.

- **Reduce Mailbox To:** Shows how many items need to be expired before the mailbox would be reduced to the size you specify. Older, larger items are expired before newer, smaller items.
- **Reduce Mailbox to Limited Size:** Shows how many items need to be expired before the mailbox is the size specified using the Disk Space Management feature. For instructions, see "Setting Mailbox Size Limits" on page 123.

When items meet your selected expire criteria, they are subject to being removed from the mailbox when you the **Expire/Reduce Messages** action. For more information, see "Reducing the Size of User and Message Databases" on page 414.

5. In the **Include** box, select **Received Items**, **Sent Items**, **Calendar Items**, **Only Backed-Up Items**, and/or **Only Retained Items** to specify the types of items to gather statistics for.

   The **Only Backed-Up Items** option interacts with the **Do Not Purge Items Until They Are Backed Up** setting under **Tools > GroupWise Utilities > Client Options > Environment Options > Cleanup**. If items are not allowed to be deleted before they are backed up, then they cannot be deleted during an Expire/Reduce operation. For more information. see "Environment Options: Cleanup" on page 555.

   The **Only Retained Items** option interacts with third-party messages retention application. For more information, see Chapter 50, "Retaining User Messages," on page 429.

6. Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

   "Databases" on page 436
   "Logging" on page 437
   "Results" on page 437
   "Misc" on page 437
   "Exclude" on page 437

   Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 437.

   By default, the mailbox statistics are sent to the domain's notification user. For more information, see "Receiving Notifications of Agent Problems" on page 242.

7. If you want to send the statistics to one or more other users, click **Results**, select **Individual Users**, specify the email addresses of the users in the **CC** field, then click **Message** if you want to include explanatory text.
8. Click **OK** to gather the mailbox statistics and email the results to the specified users.

Reducing the Size of User and Message Databases

When users archive and empty messages in their mailboxes, the messages are marked for removal from the database ("expired"), but the disk space that the expired messages occupied in the databases is retained and used again for new messages. As a result, archiving and deleting messages does not affect the overall size of the databases.

The Expire/Reduce Messages option of Mailbox/Library Maintenance enables you to expire additional messages and reduce the size of the databases by reclaiming the free space in the databases that is created when messages are expired. You can expire/reduce messages for one or more users or resources, or for all users and resources in one or more post offices. You should inform users before you run this process so they have a chance to archive or delete messages.

1. In the GroupWise Admin console, browse to and click the name of a user or resource to expire/reduce messages for them.

or

Browse to and click the name of the post office to expire/reduce messages for all users and resources in each selected post office.

2 For a user or resource, click **Maintenance**.

or

For a post office, click **Maintenance > Mailbox/Library Maintenance**.

3 From the **Actions** drop-down menu, select **Expire/Reduce Messages**.

4 Click **Reduce Only** to delete items that have already expired (that is, items that have been archived or deleted by users).

or

Click **Expire and Reduce** to expire items in addition those that users have already archived or deleted, based on the criteria you select.

Expire and Reduce: Select one or more of the following:

- **Items Older Than:** Expires items that are older than the number of days you specify.
- **Downloaded Items Older Than:** Expires items that have been downloaded to users' GroupWise Caching or Remote mailboxes that are older than the number of days you specify. It does not expire items that have been downloaded to non-GroupWise mailboxes (for example, POP and IMAP accounts).
- **Items Larger Than:** Expires items that are larger than the size you specify.
- **Trash Older Than:** Expires items in the Trash that are older than the number of days you specify.
- **Reduce Mailbox To:** Expires items until the mailbox is reduced to the size you specify. Older, larger items are expired before newer, smaller items.
- **Reduce Mailbox to Limited Size:** Expires items until the mailbox is the size specified using the Disk Space Management feature under Client Options. For more information, see "Setting Mailbox Size Limits" on page 123.

5 In the **Include** box, select **Received Items**, **Sent Items**, **Calendar Items**, **Only Backed-Up Items**, and/or **Only Retained Items**. You might want to notify users of the types of items that will be deleted.

The **Only Backed-Up Items** option interacts with the **Do Not Purge Items Until They Are Backed Up** setting under **Tools > GroupWise Utilities > Client Options > Environment Options > Cleanup**. If items are not allowed to be deleted before they are backed up, then they cannot be deleted during an Expire/Reduce operation. For more information. see "Environment Options: Cleanup" on page 555.

The **Only Retained Items** option interacts with third-party messages retention application. For more information, see Chapter 50, "Retaining User Messages," on page 429.

6 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

"Databases" on page 436
"Logging" on page 437
"Results" on page 437
"Misc" on page 437
"Exclude" on page 437

Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 437.

7 Click **Run** to perform the Expire/Reduce Messages operation.

TIP: You can also perform this task for more than one user or resource at a time by using the **Maintenance > Mailbox/Library Maintenance** dialog on the Post Office where the users or resources are located, then selecting **Maintenance on User/Resources on this Post Office**.

For additional disk space management assistance, see "Managing Disk Space Usage in the Post Office" on page 121.

Reclaiming Disk Space in Domain and Post Office Databases

As you add information to your system, the domain databases (`wpdomain.db`) and post office databases (`wphost.db`) increase in size. If you delete information, the space created in the databases for the information is not immediately recovered. GroupWise uses the free space before requiring more disk space; however, if you have deleted a large amount of information, you might want to reclaim unused database space. If you have frequent changes to your users, especially deletions, you should occasionally reclaim disk space.

1 In the GroupWise Admin console, browse to and click the name of the domain or post office where you want to reclaim disk space.

2 For a domain, click **Maintenance**.

   or

   For a post office, click **Maintenance > Post Office Database**.

3 Select **Reclaim Unused Space**.

4 Click **Run**.

   If the task takes a while to complete, see "Monitoring Background Administrative Tasks" on page 36.

Reducing the Size of Libraries and Document Storage Areas

The amount of disk space you allow at each post office for your library databases varies according to the GroupWise features they use.

If you are using GroupWise Document Management Services, you must determine storage requirements for your documents. If you feel your current disk space usage by documents is not representative of your long-term requirements, you can estimate the disk space users need for documents by multiplying an average document size by the average number of documents per user by the total number of users in the post office.

For example, the typical document size is 50 KB. Each user owns about 50 documents and there are 100 users on your post office.

Sample Calculation:

```
   50 KB (document size)
x  50 documents (per user)
x 100 users
-----
  2.5 GB of disk space
```

Be sure to allow your libraries room to grow.

When room to grow is no longer available, the following tasks help you make the best use of available disk space:

* "Archiving and Deleting Documents" on page 417
* "Deleting Activity Logs" on page 418

See also "Backing Up and Restoring Archived Documents" on page 530.

Archiving and Deleting Documents

Documents can be archived, retained indefinitely, or simply deleted. The document type property determines a document's disposition (archive, delete, or retain). The document life property determines when it can be archived or deleted. When you run the **Archive/Delete Documents** option of Mailbox/Library Maintenance, documents in the selected libraries that have reached their document life dates are either deleted or archived.

Documents that have reached their document life and been marked for deletion in the document type are simply deleted from the library, after which the document and its property information can no longer be found by any search. You can recover deleted documents from database backups.

When documents are archived, their BLOBs are moved to archive folders. These folders are named `ar`*nnnnnn* (where *nnnnnn* is an incremented integer with leading zeros), and are automatically created as needed. They are sometimes referred to as archive sets. The archive folders are located at *post_office_folder*`\gwdms\lib`*01-FF*`\archive`. When a document is archived, GroupWise determines if the document BLOB fits in the current archive folder. If the BLOB does not fit, another archive folder is created and the BLOB is archived there.

To archive/delete documents from one library or all libraries in the selected post offices:

1. In the GroupWise Admin console, browse to and click the name of the library or post office which contains the documents you want to archive/delete.
2. For a library, click **Maintenance**.

   or

   For a post office, click **Maintenance > Post Office Database**.
3. From the **Actions** drop-down menu, select **Archive/Delete Documents**.
4. Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

   "Databases" on page 436
   "Logging" on page 437
   "Results" on page 437
   "Misc" on page 437

   Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 437.
5. Click **Run** to perform the Archive/Delete Documents operation.

TIP: You can also perform this task for more than one library object at a time by using the **Maintenance > Mailbox/Library Maintenance** dialog on the Post Office where the library objects are located, then selecting **Maintenance on Libraries on this Post Office**.

Deleting Activity Logs

To free up disk space by deleting the activity logs for one or more libraries:

1 In the GroupWise Admin console, browse to and click the name of the library or post office where you want to delete activity logs.

2 For a library, click **Maintenance**.

or

For a post office, click **Maintenance > Post Office Database**.

3 From the **Actions** drop-down menu, select **Delete Activity Logs**.

4 Specify the number of days in the **Delete Activity Logs Older Than** field. The default is 60 days.

5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

“Databases” on page 436
“Logging” on page 437
“Results” on page 437
“Misc” on page 437

Selected options can be saved for repeated use. See “Saving Mailbox/Library Maintenance Options” on page 437.

6 Click **OK** to delete unneeded activity logs.

47 Troubleshooting Database Problems

The Record Enumerations tool lets you look inside your GroupWise databases to view the contents on a record-by-record basis. This is very useful for troubleshooting database issues such as checking replication between domains and GroupWise systems.

1. In the GroupWise Admin console, click **System > Record Enumerations**.
2. Select the record type that you want details about.

   For example, if you want to see all the records for a user, you could select **Users By Name**.
3. To see all of the records associated with a user, select the user, then click **Information**.
4. Click **Close** to return to the main Admin console window.

48 Backing Up GroupWise Databases

You should back up GroupWise databases regularly so that if a database sustains damage that cannot be repaired using the GroupWise database maintenance tools, you can still recover with minimum data loss.

Use your backup software of choice to back up GroupWise databases to a secure location. For a list of compatible products, see the Partner Product Guide (http://www.novell.com/partnerguide/). You can also use the GroupWise Database Copy utility (DBCopy) and the GroupWise Backup Time Stamp utility (GWTMSTMP) to assist with backups. For details about how to use these utilities, see Chapter 51, "Stand-Alone Database Maintenance Programs," on page 433.

Backing Up a Domain

All critical domain-level information is stored in the domain database (`wpdomain.db`). Use your backup software of choice to back up each domain database to a secure location. If your backup software cannot handle open files, stop the MTA for the domain while the backup of the domain database takes place or copy the domain folder to a temporary location and back up the static copy.

See also "Restoring a Domain" on page 423.

Backing Up a Post Office

Critical post office-level information is stored in many different databases. The table below summarizes the databases and their locations:

Database	Location
wphost.db	*post_office_folder*
ngwguard.db	*post_office_folder*
msg*nnn*.db	*post_office_folder*\ofmsg
user*xxx*.db	*post_office_folder*\ofuser
pu*xxxxx*.db	*post_office_folder*\ofuser
*.idx and *.inc	*post_office_folder*\ofuser\index
fd*0-F6*	*post_office_folder*\offiles
dmsh.db	*post_office_folder*\gwdms
dm*xxnn01-FF*.db	*post_office_folder*\gwdms\lib*0000-FF*
fd*0-FF*	*post_office_folder*\gwdms\lib*0000-FF*\docs
*.idx and *.inc	*post_office_folder*\gwdms\lib*0000-FF*\index

Use your backup software of choice to back up all databases in each post office to a secure location. If your backup software cannot handle open files, stop the POA for the post office while the backup of the domain database takes place or copy the post office folder to a temporary location and back up the static copy.

See also "Restoring a Post Office" on page 423.

Backing Up a Library and Its Documents

If the document storage area for a library is physically located in a post office, the library and documents are backed up along with the rest of the data in the post office. However, document storage areas are frequently located outside of the post office folder structure because of disk space considerations. Therefore, remote document storage areas must be backed up separately. A post office can have multiple libraries and each library can have multiple document storage areas, so ensure that you have identified all document storage areas in your library/document backup procedure.

After you have initially performed a full backup of your document storage areas, you can perform incremental backups by backing up to the same location to shorten the backup process.

To ensure consistency between the backups of post office databases and document storage areas:

1. Use your backup software of choice to back up your document storage areas.
2. Back up the post office.

   For instructions, see "Backing Up a Post Office" on page 421.
3. Perform an incremental backup of your document storage areas to pick up all new documents and document modifications that occurred while backing up the post office.

You should need to restore data in a document storage area only if files have been damaged or become inaccessible due to a hard disk failure.

See also "Restoring a Library" on page 424.

Backing Up Individual Databases

If you need to back up individual databases separately from backing up a post office, you can use your backup software of choice.

See also "Restoring an Individual Database" on page 425.

49 Restoring GroupWise Databases from Backup

Database damage can usually be repaired using the database maintenance tools provided with GroupWise. Only very occasionally should you need to restore databases from backup.

Restoring a Domain

Typically, damage to the domain database (`wpdomain.db`) can be repaired using the database maintenance tools provided in the GroupWise Admin console. For more information, see Chapter 42, “Maintaining Domain and Post Office Databases,” on page 395.

If damage to the domain database is so severe that rebuilding the database is not possible:

1. Stop the MTA for the domain.
2. Use the backup software for your platform to restore the domain database into the domain folder.

   For more information, see “Backing Up a Domain” on page 421.
3. Restart the MTA for the domain.
4. To update the restored domain database with administrative changes made since it was backed up, replicate information in the primary domain database to the restored domain database.

   For more information, see “Replicating Secondary Domains, Post Offices, and Libraries” on page 412

   If the restored domain database is for the primary domain, see “Synchronizing the Primary Domain from a Secondary Domain” on page 412.

Restoring a Post Office

Typically, damage to databases in a post office can be repaired using the database maintenance tools provided in the GroupWise Admin console or using GroupWise Check (GWCheck).

See the following sections for more information:

- Chapter 42, “Maintaining Domain and Post Office Databases,” on page 395
- Chapter 43, “Maintaining User/Resource and Message Databases,” on page 403
- “GroupWise Backup Time Stamp Utility” on page 444

If damage to the post office was so severe that rebuilding databases is not possible:

1. Stop the POA for the post office.
2. Use the backup software for your platform, to restore the various databases into their proper locations in the post office folder.

   For a list of backup software, see “Backing Up a Post Office” on page 421.

3 Time-stamp the restored user databases so that old items are not automatically purged during nightly maintenance:

3a In the GroupWise Admin console, browse to and click the name of the user, then click **More > Restore**,

3b Click **Yes**.

4 To update the restored post office database (`wphost.db`) with the most current information stored in the domain database, rebuild the post office database.

For instructions, see "Rebuilding Domain or Post Office Databases" on page 398.

5 To update other restored databases such as user databases (`user`*`xxx`*`.db`) and message databases (`msg`*`nnn`*`.db`) with the most current information stored in other post offices, run Analyze/Fix Databases with **Contents** selected.

For instructions, see "Analyzing and Fixing User/Resource and Message Databases" on page 403.

6 Restart the POA for the post office.

Restoring a Library

Typically, damage to library databases (`dmsh.db` and others) can be repaired using the database maintenance tools provided in the GroupWise Admin console or using GroupWise Check (GWCheck).

See the following sections for more information:

- Chapter 44, "Maintaining Library Databases and Documents," on page 407
- "GroupWise Check" on page 433

If damage to the library is so severe that rebuilding databases is not possible:

1 Stop the POA that services the library.

2 Use the backup software for your platform, to restore the library.

For a list of backup software, see "Backing Up a Library and Its Documents" on page 422

3 Restart the POA.

4 To update the restored library databases with the most current information stored in other post offices:

4a In the GroupWise Admin console, run Analyze/Fix Databases with **Contents** selected.

4b Run Analyze/Fix Library.

For more information, see "Analyzing and Fixing Library and Document Information" on page 408.

Restoring an Individual Database

Typically, damage to user and resource databases (`userxxx.db`) and message databases (`msgnnn.db`) can be repaired using the database maintenance tools provided in the GroupWise Admin console or using GroupWise Check (GWCheck).

See the following sections for more information:

- Chapter 43, “Maintaining User/Resource and Message Databases,” on page 403
- “GroupWise Check” on page 433

If damage to an individual database is so severe that repair is not possible:

1. Ensure that the user to whom the affected database belongs is not running the GroupWise client.
2. Use your backup software of choice to restore the database into the proper location in the post office folder.

   User databases are stored in the `ofuser` subfolder in the post office. Message databases are stored in the `ofmsg` subfolder.
3. To update the restored database with the most current information available, run **Analyze/Fix Databases** with **Contents** selected.

   For instructions, see “Analyzing and Fixing User/Resource and Message Databases” on page 403.

Restoring Deleted Mailbox Items

With proper planning, you can assist users in retrieving accidentally deleted items and items that became unavailable because of database damage.

- “Setting Up a Restore Area” on page 425
- “Restoring a User’s Mailbox Items” on page 427
- “Letting Client Users Restore Their Own Mailbox Items” on page 427

NOTE: Setting up a restore area enables users to restore deleted mailbox items (messages, appointments, tasks, and so on), but not deleted contacts (entries in Contacts folders and personal address books).

Setting Up a Restore Area

A restore area is only as useful as the post office data that is backed up regularly. Ensure that you are backing up every GroupWise post office regularly. For more information, see “Backing Up a Post Office” on page 421.

A restore area is a location you designate to hold a backup copy of a post office so that you or GroupWise client users can access it to retrieve mailbox items that are unavailable in your live GroupWise system.

To set up a restore area:

1. Create a backup copy of the post office folder for users to access as a restore area.

   The name of the restore area folder must follow the same conventions as a post office folder.

2 In the GroupWise Admin console, click **System > Restore Area Management**.

   The Restore Area dialog box lists any restore areas that currently exist in your GroupWise system.

3 Click **New** to set up a new restore area.

4 On the **General** tab, specify a unique name for the new restore area. If desired, provide a lengthier description to further identify the restore area.

   You can set up one restore area per post office.

5 In the **Path** field, browse to and select the folder that you created in Step 1.

   If the location is on a remote Windows server:

   5a Specify the remote location as a UNC path.

   5b Configure the POA service to run as This Account on the Windows server with administrator rights to access the remote location.

   5c (Conditional) If the remote location requires different credentials from those in use by the POA service, specify the user name and password for the remote location on the Post Office **Settings** tab.

6 (Conditional) For a restore area on Linux, specify the full path to the folder that you created in Step 1 in the **Linux Path** field in Linux path format, so that the Linux POA can locate the restore area.

7 Click the **Membership** tab.

8 Click **Add**, select the post office, or one or more individual users in the post office, that need access to the new restore area, then click **OK** to add them to the membership list.

9 When the membership list is complete, click **OK** to create the new restore area.

   If you display the Post Office **Settings** tab for a post office that has a restore area assigned to it, you see that the **Restore Area** field has been filled in.

10 Use the backup software for your platform, as listed in "Backing Up a Post Office" on page 421, to restore a backup copy of the post office into the restore area.

11 Grant the user who is starting the POA the following rights to the restore area folder:

Linux:	755
Windows:	Change

12 (Conditional) For a restore area on Windows, if the restore area is located on a different server from where the post office folder is located, provide the POA with a user name and password for logging in to the remote server.

   You can provide that information using the **Remote User Name** and **Password** fields on the Post Office **Settings** tab, or using the /user and /password startup switches.

13 Continue with "Restoring a User's Mailbox Items" on page 427 or "Letting Client Users Restore Their Own Mailbox Items" on page 427 as needed.

Restoring a User's Mailbox Items

After you have set up a restore area and placed a backup copy of a post office into it, you can restore a user's mailbox items for the user.

1. In the GroupWise Admin console, browse to and click the name of a user or resource for which you need to restore mailbox items.
2. Click **More > Restore**.
3. Click **Yes** to restore the user's or resource's mailbox items.
4. Notify the user and explain the following about the restored items:
   - The user might want to manually delete unwanted restored items.
   - The user should file or archive the items that he or she wants within seven days. After seven days, unaccessed items are deleted after the amount of time allowed by existing auto-delete settings. For details, see "Environment Options: Cleanup" on page 555. If auto-deletion is not enabled, the restored items remain in the mailbox indefinitely.

Letting Client Users Restore Their Own Mailbox Items

After you have set up a restore area and given client users access to it, users can selectively restore individual items into their mailboxes. This saves you the work of restoring mailbox items for users and it also saves users the work of deleting unwanted restored items.

In the backup copy of a mailbox, only items that are different from the live mailbox are displayed. If the backup mailbox looks empty, it means that it matches the contents of the live mailbox.

After a restore area has been set up:

1. In the GroupWise client, click **File > Open Backup**.
2. (Conditional) If you are prompted:
   - **2a** In the **Restore From** field, browse to and select the restore area folder.
   - **2b** In the **Password** field, type your GroupWise password.
   - **2c** Click **OK** to access the backup copy of your mailbox.
3. Retrieve individual items as needed.

   The backup copy of your mailbox offers basic features such as Read, Search, and Undelete so that you can locate and retrieve the items you need.
4. When you are finished restoring items to your live mailbox, click **File > Open Backup** again to remove the check mark from the **Open Backup** option and return to your live mailbox.

Recovering Deleted GroupWise Accounts

If you have a reliable backup procedure in place, you can restore recently deleted GroupWise user and resource accounts. For more information, see Chapter 48, "Backing Up GroupWise Databases," on page 421.

1. Make available a backup copy of a domain database (`wpdomain.db`) where the deleted GroupWise account still exists.
2. In the GroupWise Admin console, click **System > Recover Deleted Account**.
3. Browse to and select the backup copy of the domain database.
4. Click **Account to Recover**, select the user or resource that you need to recover the account for, then click **OK**.

   At this point, you have restored the user's or resource's GroupWise account into the GroupWise system. However, this does not restore ownership of resources, nor does the account's mailbox contain any item at this point.
5. If the restored user owned resources, manually restore the ownership.

   For instructions, see "Changing a Resource's Owner" on page 498.
6. Restore the contents of the account's mailbox.

   For instructions, see "Restoring Deleted Mailbox Items" on page 425.

50 Retaining User Messages

GroupWise enables you to retain user messages until they have been copied from message databases to another storage location. This means that a user cannot perform any action, such as emptying the mailbox Trash, that results in a message being removed from the message database before it has been copied.

Message retention primarily consists of three activities:

- Not allowing users to remove messages until they have been retained.
- Retaining the messages by copying them from message databases to another location.
- Time-stamping the retained messages so that they can be subsequently deleted.

GroupWise supplies the ability to not allow users to remove messages until they have been retained. It also provides methods for message retention applications to securely access user mailboxes and copy messages. However, it does not provide the message retention application. You must develop or purchase a third-party (non-GroupWise) application that performs this service.

How Message Retention Works

To understand how message retention works, you need to understand what GroupWise does and what the message retention application does.

What GroupWise Does

During installation of the message retention application, the application uses the GroupWise Trusted Application API to create a trusted application record in the GroupWise system. The trusted application record includes a flag that designates it as a message retention application. This flag is accessed through the trusted application’s **Provides Message Retention Service** setting (GroupWise Admin console > **System > Trusted Applications > Edit**).

When the GroupWise Admin console reads a trusted application record that has the **Provides Message Retention Service** setting enabled, it adds the Message Retention Service to the **Retention** tab in the Environment Options (GroupWise Admin console > Domain object, Post Office object, or User object > **Client Options > Environment > Integrations > Retention**).

You use this **Retention** tab to enable message retention at the domain, post office, or user level, meaning that you can enable it for all users in a domain, all users in a post office, or individual users.

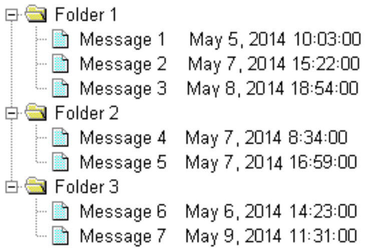
Enabling message retention alters the GroupWise client purge behavior by preventing a user from purging any messages from his or her mailbox that have not yet been retained.

What the Message Retention Application Does

Different message retention applications might vary slightly in their approach to retaining messages. This section provides a general approach to message retention.

To determine whether or not mailbox messages have been retained, the message retention application adds a time stamp to the mailbox. The message retention application can use the GroupWise Object API or GroupWise IMAP support to write (and read) the time stamp. In the GroupWise Admin console, you can click **More > Time Stamp** on an object in order to apply a basic time stamp. In addition, you can use the GroupWise Backup Time Stamp Utility to manually set the time stamp. For more information, see "GroupWise Backup Time Stamp Utility" on page 444.

The time stamp represents the most recent date and time that message retention was completed for the mailbox. Messages delivered after the time stamp cannot be purged until they have been retained. This requires that the message retention application retain items chronologically, oldest to newest. For example, assume a mailbox has a message retention time stamp of May 7, 18 12:00:00. The mailbox has three folders with a total of seven messages:



The message retention application reads the existing time stamp (May 7, 18 12:00:00) and selects a time between that time and the current time. For example, suppose the current time is May 9, 18 14:00:00. The message retention application could choose May 8, 18 12:00:00 as the new time stamp. It would then retain any messages delivered between the existing time stamp (May 7, 18 12:00:00) and the new time stamp (May 8, 18, 12:00:00).

In the above example, messages 1, 4, and 6 are older than the existing time stamp (May 7, 18 12:00:00). The message retention application would not retain these messages again, assuming that they had already been safely retained. Messages 2 and 5 have dates that fall between the existing time stamp (May 7, 18 12:00:00) and the new time stamp (May 8, 18, 12:00:00) so they would be retained. Messages 3 and 7 have dates that fall after the new time stamp (May 8, 18, 12:00:00) so they would not be retained until the next time the message retention application ran against the mailbox.

Optionally, the message retention service can be associated with an archive service. For more information, see "Archive Service Settings" on page 60.

Acquiring a Message Retention Application

If you do not already have a message retention application to use with GroupWise, you have two options:

- Purchase an application from a GroupWise partner.

  For information about GroupWise partners that provide message (email) retention applications, see the Partner Product Guide (http://www.novell.com/partnerguide/).

* Develop your own application.

  For information about developing a message retention application, see the *GroupWise Object API* and *GroupWise Trusted Application API* documentation at the GroupWise for Software Developers website (https://www.novell.com/developer/ndk/groupwise/develop_to_groupwise.html).

Enabling Message Retention

This section assumes that you have installed a message retention application as a GroupWise trusted application and that it is configured to provide a message retention service. If not, see “Trusted Applications” on page 64.

Message retention is not enabled until you designate the users whose messages you want retained by the application. You can designate users at the domain level, post office level, or individual user level.

1. In the GroupWise Admin console, browse to and click the name of the domain, post office, or user for which you want to enable message retention.
2. Click **Client Options** to display the GroupWise Client Options dialog box.
3. Click the **Integrations** tab, then click **Retention**.
4. Select **Enable Message Retention Service**.
5. (Conditional) If you want to lock the setting at this level, click the **Lock** button.

   For example, if you lock the setting at the domain level, the setting cannot be changed for any post offices or users within the domain. If you lock the setting at the post office level, it cannot be changed individually for the post office’s users.

   This setting does not display in the GroupWise client. Therefore, there is no lock available when editing this setting for individual users.
6. Click **OK** to save the changes.

51 Stand-Alone Database Maintenance Programs

Some aspects of GroupWise database maintenance are performed by stand-alone maintenance programs that can be incorporated into batch files along with other system maintenance programs.

GroupWise Check

GroupWise Check (GWCheck) is a tool provided for GroupWise to check and repair GroupWise user, message, library, and resource databases without needing the Admin console. In addition to checking and repairing databases in the post office, it also checks and repairs users' remote, caching, and archive databases on user workstations or other personal locations.

The GWCheck utility runs on Linux and Windows. You should match the platform of GWCheck to the platform where the databases are located. Linux GWCheck processes databases on Linux. Windows GWCheck processes databases on Windows.

IMPORTANT: GWCheck should not be used to process databases that are located across a network connection between different machines.

GWCheck Functionality

The GWCheck utility begins by comparing three databases.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
The post office database (`wphost.db`) is checked for the file ID (FID) of the selected user.	The guardian database (`ngwguard.db`) is checked to find out if this user database has been created.	The file system for this post office is checked to see if the user database (`user`*`xxx`*`.db`) for this user exists.

After GWCheck makes the database comparisons, it begins processing according to the databases selected and any inconsistencies found.

Case 1 - Missing Entry in the Post Office Database (wphost.db)

In this example, a contents check is run either against all users on the post office or against one user, "ABC." GWCheck does not find the FID of one or more users.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
?	userabc.db	userabc.db
No entry for this user is found in the post office database (`wphost.db`).	An entry is found in the guardian database (`ngwguard.db`), indicating that the user has been deleted.	Also, a user database (`user`*`xxx`*`.db`) for this user is found in the ofuser folder.

GWCheck removes the entry from `ngwguard.db,` deletes `userabc.db`, and systematically deletes all of the user's messages from the message databases that are not still being referenced by other users. If the user has been deleted, GWCheck cleans up after that user.

WARNING: If a post office database becomes damaged so some users are unable to log in, GWCheck should not be run until the post office has been rebuilt. For more information, see "Rebuilding Domain or Post Office Databases" on page 398.

Case 2 - Missing Entry in the Guardian Database (ngwguard.db)

In this example, a GWCheck is run either against all users on the post office or against one user, "ABC." A user's FID is found and the user's database is found in the post office, but the user is missing in `ngwguard.db`.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
FID abc	?	userabc.db
The user appears in the post office database (`wphost.db`).	The guardian database (`ngwguard.db`) shows no user database for this user.	A user database (`user`*`xxx`*`.db`) for the user does exist in the ofuser folder.

GWCheck creates the user in `ngwguard.db`, using database `userabc.db`. Even if `ngwguard.db` is damaged, it is unlikely that data is lost.

Case 3 - Missing User Database (user*xxx*.db)

In this example, a GWCheck is run either against all users on the post office or against one user, "ABC." The user's FID is found, as well as the user's record in `ngwguard.db`. However, the user's database is not found.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
FID abc	userabc.db	?
The user is found in the post office database (`wphost.db`).	The user is found in the guardian database (`ngwguard.db`).	No user database (`user`*`xxx`*`.db`) is found in the ofuser folder.

GWCheck takes action depending on what options are selected.

Contents Check: GWCheck deletes all of this user's messages from the message databases if they are not referenced by other users.

Structural Rebuild: GWCheck creates a blank user database for this user. Existing messages for this user are ignored.

Re-create User Database: GWCheck creates a blank user database for this user and populates it with messages in the message databases that have been sent to or from this user.

WARNING: If a user database has been deleted, do not run a Contents Check until after a Structural Rebuild or Re-create User Database has been run for that user. For more information, see "Performing a Structural Rebuild of a User/Resource Database" on page 405 and "Re-creating a User/Resource Database" on page 406.

Using GWCheck on Linux

Two versions of GWCheck are available on Linux, one for a graphical user interface (GUI) environment and one for a text-only environment.

- "Using GUI GWCheck (gwcheck)" on page 435
- "Using Text-Based GWCheck (gwcheckt)" on page 435

Using GUI GWCheck (gwcheck)

1 Change to the `/opt/novell/groupwise/agents/bin` folder.

2 Enter `./gwcheck` to start GWCheck.

3 Continue with Performing Mailbox/Library Maintenance Using GWCheck.

Using Text-Based GWCheck (gwcheckt)

You can use text-based GWCheck in any environment where the X Window System is not available, such as on a text-only server where a post office and its POA are located. However, you must use GUI GWCheck to create an options file before you can run text-based GWCheck.

1 Run GUI GWCheck in a convenient location.

For instructions, see "Using GUI GWCheck (gwcheck)" on page 435

2 Select the maintenance activities that you want GWCheck to perform.

For instructions, see "Performing Mailbox/Library Maintenance Using GWCheck" on page 436.

3 Save the settings you selected in an options file.

The default options file name is `gwcheck.opt`.

For instructions, see "Saving Mailbox/Library Maintenance Options" on page 437.

4 Copy the GWCheck options file you created in Step 3 to the `/opt/novell/groupwise/agents/bin` folder.

5 Change to the `/opt/novell/groupwise/agents/bin` folder.

6 Enter `./gwcheckt` *`options_file_name`* to run text-based GWCheck.

Over time, a collection of options files might accumulate. To see what maintenance activities an options file performs, use `./gwcheckt` *`options_file_name`* `--dump`.

To remind yourself of these options when you are at your Linux server, view the gwcheckt man page.

Using GWCheck on Windows

You can use GWCheck in any supported Windows environment. See the following sections for current system requirements:

- Windows servers: "Hardware and Operating System Requirements"
- Windows workstations: "GroupWise Client User Requirements"

As an administrator, you can run GWCheck for databases in any post office accessible from the workstation where GWCheck is installed. The GWCheck program performs all database maintenance itself, rather than handing off a task to the POA as the GroupWise Admin console would do to perform database maintenance.

Depending on how GWCheck is installed, users can have a **Repair Mailbox** item on the GroupWise client **Tools** menu that enables them to run GWCheck from the client. If the GWCheck program is available to users, users can perform database maintenance on their Remote, Caching, and archive mailboxes, which are not accessible from the GroupWise Admin console.

For the **Repair Mailbox** item to display on the GroupWise client **Tools** menu, the following files must be installed in the GroupWise software folder:

- `gwcheck.exe`
- `gwchk`*`xx`*`.dll` (Replace *xx* with your language code)
- `gwchk`*`xx`*`.chm` (Replace *xx* with your language code)

The default location for the GroupWise software is `c:\Program Files\Micro Focus\GroupWise`.

To run GWCheck:

1. From the **Start** menu, click **Run**, then browse to and double-click `gwcheck.exe`.
2. Continue with "Performing Mailbox/Library Maintenance Using GWCheck" on page 436.

Performing Mailbox/Library Maintenance Using GWCheck

With only a few differences in interface functionality, as described in the online help, you can perform the same maintenance activities in GWCheck as you can in Mailbox/Library Maintenance in the GroupWise Admin console:

- "Using Mailbox/Library Maintenance Tab Options" on page 436
- "Reusing Mailbox/Library Maintenance Settings" on page 437

Using Mailbox/Library Maintenance Tab Options

Both GWCheck and Mailbox/Library Maintenance in the GroupWise Admin console use tab options to control the checking process.

- "Databases" on page 436
- "Logging" on page 437
- "Results" on page 437
- "Misc" on page 437
- "Exclude" on page 437

Databases

To select the types of database to perform the Mailbox/Library Maintenance check on, click **Databases**.

Depending on the object type and action already selected in the main window, some database types might be unavailable. If all the database types are unavailable, then one or more database types have been preselected for you.

You can perform an action on the following databases when the type is not unavailable:

- **User:** Checks the user databases.
- **Message Databases:** Checks the message databases.
- **Document:** Checks the library and document properties databases.

Logging

To specify the name of the file where you want the results of the MailBox/Library Maintenance check to be stored, click **Logging**.

Specify a file name. By default, the file is created in the home folder of the user who is running GWCheck. Specify a full path to create the log file in a different location.

Click **Verbose Logging** to log detailed information. Verbose logging might produce large log files and slow execution.

This file is sent to the users selected on the **Results** tab.

Results

To select users to receive the results of the Mailbox/Library Maintenance check, click **Results**.

Select **Administrator** to send the results to the user defined as the GroupWise domain's notification user. For more information, see "Receiving Notifications of Agent Problems" on page 242.

Select **Individual Users** to send each user the results that pertain to him or her. Specify each user's GroupWise user name or email address in a comma-delimited list. Click **Message** to include a customized message with the results file.

Misc

If you need to run a Mailbox/Library Maintenance check with special options provided by Micro Focus Support, click **Misc**.

Use the **Support Options** field to specify command line parameters. Support options are typically obtained from Micro Focus Support representatives when you need assistance resolving specific database problems. Search the Micro Focus Support Knowledgebase (http://www.novell.com/support/) for TIDs and Support Pack Readmes that list support options. Ensure that you clearly understand what the Support options do before you use them.

Exclude

If you want to exclude certain users in the selected post office from having the Mailbox/Library Maintenance check performed on their databases, click **Exclude**.

Click **Add**, select one or more users to exclude, then click **OK**.

Reusing Mailbox/Library Maintenance Settings

For convenience, you can store the options you select in Mailbox/Library Maintenance and GWCheck so that you can retrieve them for later use.

- "Saving Mailbox/Library Maintenance Options" on page 437
- "Retrieving Mailbox/Library Maintenance Options" on page 438

Saving Mailbox/Library Maintenance Options

1. After you have selected all of the options in the **Mailbox/Library Maintenance** dialog box, click **Save**.
2. Browse to the folder where you want to save the options file.

   You might want to save it in the domain folder to which you are currently connected.

3 Specify a file name if you do not want to use the default of `gwcheck.opt`.

4 Click **Save**.

The GWCheck options file is created in XML format on all platforms. Therefore, you can create the GWCheck options file on any platform and use it on any platform interchangeably.

Retrieving Mailbox/Library Maintenance Options

1 In the **Mailbox/Library Maintenance** dialog box, click **Retrieve**.

2 Browse to and select your saved options file.

3 Click **Open**.

Executing GWCheck from a Linux Script

The GWCheck program is located in the following folder:

```
/opt/novell/groupwise/agents/bin
```

1 Create a script to execute GWCheck using the following syntax:

```
/opt/novell/groupwise/agents/bin/gwcheck --opt=options_file --batch
```

2 To create an options file, see "Saving Mailbox/Library Maintenance Options" on page 437.

Executing GWCheck from a Windows Batch File

The GWCheck program is located in the following folder:

```
c:\Program Files\Micro Focus\GroupWise Server\agents\gwcheck
```

It is also installed along with the GroupWise client software in the `gwcheck` subfolder of the GroupWise client installation folder.

1 Use the following syntax to create a batch file to execute GWCheck:

```
gwcheck /opt=options_file /batch
```

2 To create an options file, see "Saving Mailbox/Library Maintenance Options" on page 437.

GWCheck Startup Switches

The following startup switches can be used with GWCheck:

Linux GWCheck	Windows GWCheck
--batch	/batch
--lang	/lang
--opt	/opt
--pa	/pa
--po	/po
--pr	/pr

--batch

Runs GWCheck in the background, without a user interface. Use an options file to specify the database repair options.

	Linux GWCheck	Windows GWCheck
Syntax:	--batch	/batch

For example, to specify that you want GWCheck to run it batch mode, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --batch`

Windows: `gwcheck.exe /opt=gwcheck.opt /batch`

--lang

Specifies the language to run GWCheck in, using a two-letter language code. You must install GWCheck in the selected language in order for it to display in the selected language.

	Linux GWCheck	Windows GWCheck
Syntax:	--lang=*language_code*	/lang=*language_code*

For a list of current language codes, see Chapter 7, “Multilingual GroupWise Systems,” on page 85.

For example, to specify that you want GWCheck to run in Spanish, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --lang=es`

Windows: `gwcheck.exe /opt=gwcheck.opt /lang=es`

--opt

Specifies a database maintenance options file created in a GWCheck session. This starts GWCheck with the same options settings as the session in which the options file was created.

The default location of the options file varies by platform:

Linux: User’s home folder

Windows: Folder where `gwcheck.exe` is installed.

If the options file is not in the default folder, you must specify the full path name.

	Linux GWCheck	Windows GWCheck
Syntax:	--opt=*file_name*	/opt=*file_name*

For example, to start GWCheck with saved settings, you would use:

Linux: `./gwcheck --opt=gwcheck.opt ./gwcheck --opt=/gwsystem/post1/gwcheck.opt`

Windows: `gwcheck.exe /opt=gwcheck.opt gwcheck.exe /opt=\gwsystem\post1\gwcheck.opt`

--pa

Specifies the path to the archive folder.

	Linux GWCheck	Windows GWCheck
Syntax:	--pa=*path_to_archive*	/pa=*path_to_archive*

For example, to specify the archive database that a user keeps is his or her home folder, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --batch --pa=/home/gsmith\of7bharc`

Windows: `gwcheck.exe /opt=gwcheck.opt /batch /pa=\home\gsmith\of7bharc`

--po

Specifies the path to the post office folder.

	Linux GWCheck	Windows GWCheck
Syntax:	--po=*path_to_post_office*	/po=*path_to_post_office*

For example, to specify a post office folder, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --batch --po=/mail/sales`

Windows: `gwcheck.exe /opt=gwcheck.opt /batch /po=\mail\sales`

--pr

Specifies the path to the remote mailbox folder.

	Linux GWCheck	Windows GWCheck
Syntax:	--pr=*path_to_mailbox*	/pr=*path_to_mailbox*

For example, to specify the Remote mailbox that a user keeps on a computer at home, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --pr=/novell/groupwise\of7bharc`

Windows: `gwcheck.exe /opt=gwcheck.opt /pr=\novell\groupwise\of7bharc`

GroupWise Database Copy Utility

You can use the GroupWise Database Copy Utility (DBCopy) to back up your GroupWise system if you would prefer not to purchase a third-party backup solution. For more information, see Chapter 48, “Backing Up GroupWise Databases,” on page 421.

IMPORTANT: If you want to move domains and post offices from NetWare or Windows to Linux, see the *GroupWise Server Migration Guide*. The migration process includes DBCopy startup switches that are not described in this *GroupWise 18 Administration Guide* because they are used only for migration.

DBCopy Functionality

The GroupWise Database Copy utility (DBCopy) copies files from a live GroupWise post office or domain to a static location for backup. During the copy process, DBCopy prevents the files from being modified, using the same locking mechanism used by other GroupWise programs that access databases. This ensures that the backed-up versions are consistent with the originals even when large databases take a substantial amount of time to copy.

DBCopy is a multi-threaded application that provides highly efficient copying of large quantities of data.

DBCopy copies only GroupWise-recognized folders and files in domain and post office folders. DBCopy does not copy some folders:

- Post office queue folders (`wpcsin` and `wpcsout`): Only post office data files and folders are copied. Queue folders are not copied.
- All domain subfolders: Only domain files are copied. Queue folders are not copied.
- All subfolders under each GWIA folder in `wpgate`: Only GWIA files are copied from each GWIA folder. Queue folders of GWIA folders are not copied. For example, under `gwia`, GWIA files are copied, but no GWIA subfolders are copied.

When planning disk space for your backups, you should plan to have at least three times the size of a post office. This accommodates the post office itself, the backup of the post office, and extra space for subsequent growth of the post office.

Typically, domains grow less than post offices, so domain backups should occupy somewhat less disk space.

Using DBCopy on Linux

1. Change to the following folder:

   `/opt/novell/groupwise/agents/bin`

2. Use the following command to back up a post office:

   `./dbcopy /post_office_folder /destination_folder`

   or

   Use the following command to back up a domain:

   `./dbcopy /domain_folder /destination_folder`

   or

Use the following command to back up a remote document storage area:

```
./dbcopy -b /storage_area_folder /destination_folder
```

You can include the -i switch in any of these commands to provide the date (*mm-dd-yyyy*) of the previous copy. This causes DBCopy to copy only files that have been modified since the previous copy, like an incremental backup.

To remind yourself of these options when you are at your Linux server, view the dbcopy man page.

DBCopy creates a log file named `mmddgwbk.nnn`. The first four characters represent the date. A three-digit extension allows for multiple log files created on the same day. The log file is created at the root of the destination folder. Include the -v switch in the `dbcopy` command to enable verbose logging for the backup.

3. After DBCopy has finished copying the post office, domain, or remote document storage area, use your backup software of choice to back up the static copy of the data.
4. After the backup has finished, delete the static copy of the data to conserve disk space.

You might find it helpful to set up a cron job to run DBCopy regularly at a time of day when your system is not busy.

IMPORTANT: If you are planning on running dbcopy in a script outside of the `/opt/novell/groupwise/agent/bin` directory, then you need to add the following export to your script:

```
export LD_LIBRARY_PATH=/opt/novell/groupwise/agents/lib
```

Using DBCopy on Windows

1. At a command prompt, change to the folder where you installed the GroupWise agents (typically `c:\Program Files\Micro Focus\GroupWise Server\Agents`).
2. Use the following command to back up a post office:

```
dbcopy.exe \post_office_folder \destination_folder
```

or

Use the following command to back up a domain:

```
dbcopy.exe \domain_folder \destination_folder
```

or

Use the following command to back up a remote document storage area:

```
dbcopy.exe /b \storage_area_folder \destination_folder
```

You can include the /i switch in any of these commands to provide the date (*mm-dd-yyyy*) of the previous copy. This causes DBCopy to copy only files that have been modified since the previous copy, like an incremental backup.

DBCopy creates a log file named `mmddgwbk.nnn`. The first four characters represent the date. A three-digit extension allows for multiple log files created on the same day. The log file is created at the root of the destination folder. Include the /v switch in the `dbcopy` command to enable verbose logging for the backup.

3. After DBCopy has finished copying the post office, domain, or remote document storage area, use your backup software of choice to back up the static copy of the data.
4. After the backup has finished, delete the static copy of the data to conserve disk space.

Using DBCopy Startup Switches

The following startup switches can be used with DBCopy when you are preparing to back up GroupWise data:

Linux DBCopy	Windows DBCopy	Explanation
--b	/b	Backup of BLOB files in a document storage area
-i	/i	Incremental backup
-j	/j	DBCopy priority control
-t	/t	Number of threads
-v	/v	Verbose logging
-w	/w	Continuous logging to the screen

-b

Indicates that DBCopy is copying a document storage area, which includes BLOB (binary large object) files. Use this switch only when you need to copy BLOB files.

-i

Specifies the date of the previous copy of the data. This causes DBCopy to copy only files that have the specified date or newer, such as an incremental backup. There is no default date; you must specify a date or an increment backward from today. Valid increments are -1 to -31.

	Linux DBCopy	Windows DBCopy
Syntax:	-i *mm-dd-yyyy*	/i *mm-dd-yyyy*
	-i -*days*	/i -*days*
Example:	-i 5-18-18	/i 10-30-2015
	-i -1	/i -7

-j

Raises the priority of DBCopy processing. By default, if DBCopy detects that a POA is running, it lowers its own priority so that it does not interfere with POA processing. If DBCopy runs at night, when GroupWise users are not active, use the -j switch so that DBCopy does not lower its own priority. This speeds up DBCopy processing.

-t

Specifies the number of threads for DBCopy to start for copying data. The default number of threads is 5. Valid values range from 1 to 10.

	Linux DBCopy	Windows DBCopy
Syntax:	-t *number*	/t *number*
Example:	-t 10	/t 10

-v

Turns on verbose logging, which provides more detail than the default of normal logging. DBCopy creates a log file named `mmddgwbk.nnn`. The first four characters represent the date. A three-digit extension allows for multiple log files created on the same day. The log file is created at the root of the destination domain, post office, or document storage area folder. In addition to status and error messages, it lists any remote document storage areas associated with a post office.

-w

Turns on continuous logging to the screen.

GroupWise Backup Time Stamp Utility

You can use the GroupWise Backup Time Stamp (GWTMSTMP) utility to ensure that GroupWise user databases include the dates when they were last backed up, restored, and retained.

The following sections provide information about the utility:

GWTMSTMP Functionality

The GroupWise Backup Time Stamp utility (GWTMSTMP) places date and time information on user databases (`userxxx.db`) in order to support message backup, restore, and retention. The time stamp indicates the last time the database was backed up.

If a user deletes an item from his or her mailbox and purges it from the Trash, the item is removed from the user's database only if the time stamp shows that the item has already been backed up. Otherwise, the item remains in the user's database until the database is backed up, at which time it is purged from the database.

You can run GWTMSTMP on all user databases in a post office or on a single user database. No other databases are affected.

Backup

To ensure thorough user database backups, you can ensure that deleted items are not purged from users' databases until they have been backed up. Two conditions must be met in order to provide this level of protection against loss of deleted items:

- The **Do Not Purge Items Until They Are Backed Up** option must be selected for the post office in the Admin console (**post_office_object > Client Options > Environment > Cleanup**).
- User databases (`userxxx.db`) must be time-stamped every time a backup is performed so that items can be purged only after they are backed up.

For more information, see "Environment Options: Cleanup" on page 555.

Restore

You can use GWTMSTMP to manually add the restore time stamp to the database. The restore time stamp is not required for any GroupWise feature to work properly. Its primary purpose is informational.

Retention

If you use a message retention application, the application should automatically add the retention time stamp after retaining the database's messages. Any messages with dates that are newer than the retention time stamp cannot be purged from the database. You can use GWTMSTMP to manually add a retention time stamp.

For more information, see Chapter 50, "Retaining User Messages," on page 429.

Modified Retention

If you use a message retention application, you might need to retain items more than once if you want to capture changes to personal subjects and personal attachments on items. You can use GWTMSTMP to manually update the retention time stamp on modified items, so that they are retained again.

Running GWTMSTMP on Linux

The GWTMSTMP executable (`gwtmstmp`) is installed into the `bin` and `lib` subfolders of `/opt/novell/groupwise/agents` along with the GroupWise agents. You can copy it to additional locations if needed.

To check the existing time stamp on all GroupWise user databases in a post office, use the following command:

Syntax:

```
./gwtmstmp -p /post_office_folder
```

Example:

```
./gwtmstmp -p /gwsystem/acct
```

The results are displayed on the screen.

To set a current time stamp on all user databases in a post office, use the following command:

Syntax:

```
./gwtmstmp -p /post_office_folder --set
```

Example:

```
./gwtmstmp -p /gwsystem/acct --set
```

More specialized functionality is provided through additional GWTMSTMP startup switches. See "GWTMSTMP Startup Switches" on page 446.

To remind yourself of these options when you are at your Linux server, view the gwtmstmp man page.

Running GWTMSTMP on Windows

The GWTMSTMP program file (`gwtmstmp.exe`) is installed into the same folder where you installed the GroupWise agents. You can copy it to additional locations if needed.

To check the existing time stamp on all GroupWise user databases in a post office, use the following command:

Syntax:

```
gwtmstmp.exe /p-drive:\post_office_folder
```

Example:

```
gwtmstmp.exe /p-m:\gwsystem\acct
```

The results are displayed on the screen

To set a current time stamp on all user databases in a post office, use the following command:

Syntax:

```
gwtmstmp.exe /p-drive:\post_office_folder /set
```

Example:

```
gwtmstmp.exe /p-m:\gwsystem\acct /set
```

More specialized functionality is provided through additional GWTMSTMP startup switches.

GWTMSTMP Startup Switches

The following startup switches can be used with GWTMSTMP:

Linux GWTMSTMP	Windows GWTMSTMP
-p	/p
--backup or -b	/backup
--restore or -r	/restore
--retention or - n	/retention
--modifiedretention or -mn	/modifiedretention
--get or -g	/get
--set or -s	/set
--clear or -c	/clear
--date or -d	/date
--time or -t	/time
--gmttime or -m	/gmttime
--userid or -u	/u
--userdb or -e	/userdb

-p

(Required) Specifies the full path to the post office folder where the user databases to time-stamp are located.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	-p */post_office_dir*	/p-*drive*:*post_office_dir*
Example:	-p /gwsystem/dev	/p-j:\dev

--backup, --restore, --retention, and --modifiedretention

Specifies the type of time stamp (backup, restore, retention, or modified retention) on which to perform the get or set operation. If no time stamp type is specified, the operation is performed on the backup time stamp. Multiple time stamp types can be specified.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	--backup -b --restore -r --retention -n --modifiedretention -mn	/backup /restore /retention /modifiedretention

For example, to set the restore time stamp, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --restore --set`

Windows: `gwtmstmp /p-j:\dev /restore /set`

--get

Lists existing backup, restore, and retention time stamp information for user databases. If no time stamps are set, no times are displayed. If no other operational switch is used, --get is assumed.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	--get -g	/get

For example:

Linux: `./gwtmstmp -p /gwsystem/dev --get`

Windows: `gwtmstmp /p-j:\dev /get`

The following example returns the same results as the above example because --get is assumed:

Linux: `./gwtmstmp -p /gwsystem/dev`

Windows: `gwtmstmp /p-j:\dev`

--set

Sets the current date and time (of backup, restore, or retention) on user databases.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	--set -s	/set

For example, to set the backup time stamp, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --backup --set`

Windows: `gwtmstmp /p-j:\dev /backup /set`

or

Linux: `./gwtmstmp -p /gwsystem/dev --set`

Windows: `gwtmstmp /p-j:\dev /set`

--clear

Removes time stamps (of backup, restore, or retention) from user databases.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	--clear -c	/clear

For example, to clear all time stamps on databases in a post office, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --clear`

Windows: `gwtmstmp /p-j:\dev /clear`

--date

Specifies the date that you want placed on user databases. If no date is specified, the current date is used.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	--date *mm/dd/yyyy* -d *mm/dd/yyyy*	/date-*mm/dd/yyyy*
Example:	--date 05/18/18 -d 05/18/18	/date-04/12/18

For example, to set the restore date to June 15, 18, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --restore --date 06/15/18`

Windows: `gwtmstmp /p-j:\dev /restore /date-06/14/18`

--time

Specifies the time that you want placed on user databases. If no time is specified, 00:00 is used.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	--time *hh*:*mm* am|pm -t *hh*:*mm* am|pm	/time-*hh*:*mm* am|pm
Example:	--time 2:00am -t 2:00am	/time-6:15pm

For example, to set the restore time to 4:45 p.m., you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --restore --time 4:45pm`

Windows: `gwtmstmp /p-j:\dev /restore /time-4:45pm`

--gmttime

Specifies the number of seconds since midnight on January 1, 1970 Greenwich Mean Time (GMT), that you want placed on the user databases.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	--gmttime *seconds* -m *seconds*	/gmttime-*seconds*

--userid

Provides a specific GroupWise user name so that an individual user database can be time-stamped.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	--userid *userID* -u *user_name*	/u-*user_name*
Example:	---userid gsmith -u gsmith	/u-mbarnard

For example, to set the retention time stamp for a user whose GroupWise user name is mpalu, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --userid mpalu --retention --set`

Windows: `gwtmstmp /p-j:\dev /u-mpalu /retention /set`

--userdb

Provides a specific user database (`user`*`xxx`*`.db`) so that an individual user database can be time-stamped.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	--userdb *user_database* -e *user_database*	/userdb *user_database*
Example:	--userdb user3gh.db	/userdb user3gh.db

For example, to set the retention time stamp for a user whose user database is named user3gh, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --userdb user3gh.db --retention --set`

Windows: `gwtmstmp /p-j:\dev /userdb user3gh.db /retention /set`

IX Users

52 Creating GroupWise Accounts

For users to be able to use GroupWise, you must give them GroupWise accounts. A GroupWise account defines the user in the GroupWise system by providing the user with a GroupWise user name and mailbox.

You can give GroupWise accounts to users during or after their creation in an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory. You can also give GroupWise accounts to users who do not have LDAP accounts.

Establishing a Default Password for All New GroupWise Accounts

To save time and energy when you are creating new GroupWise accounts, you can establish a default password to use for all new accounts.

1. In the GroupWise Admin console, click **System** > **System Preferences** and locate the **Default Password** section.
2. Type the password you want to use as the default, then click **OK**.
3. Explain to users how to set their own passwords in GroupWise, as described in:
   - "Assigning a Password to Your Mailbox" in the *GroupWise 18 Client User Guide*
   - "Changing Your Password" in the *GroupWise 18 WebAccess User Guide*

   NOTE: Users cannot change their passwords in GroupWise WebAccess Mobile on tablet devices.

Creating GroupWise Accounts by Importing Users from an LDAP Directory

Users are imported into your GroupWise system one post office at a time. The post office must already exist. Users are imported based on the context of their User objects in the LDAP directory.

1. In the GroupWise Admin console, configure your GroupWise system to communicate with the LDAP directory.

   For instructions, see "Setting Up an LDAP Directory" on page 79.
2. Click **System > User Import**.
3. (Conditional) If you have multiple LDAP directories, select the one from which you want to import the GroupWise users.
4. Select the post office into which you want to import the users.
5. (Conditional) If the context of the User objects is under the Base DN, browse to and select the LDAP context where User objects are located.

6 (Optional) Specify an LDAP filter and select additional options as needed.

7 (Optional) Select **Import User Photo** to import the user photo stored in the directory to the GroupWise System Address Book.

8 Click **Preview** to list the users who will be imported into GroupWise from the LDAP directory.

9 (Conditional) As needed, adjust the filter and options, then click **Update Preview** until you are satisfied with the list.

10 Click **Import Users**.

11 Click **Close** to close the User Import dialog box.

The users are given GroupWise mailbox in the post office you selected and can access their mailboxes through the GroupWise client or GroupWise WebAccess.

12 (Conditional) If you receive an error indicating that the LDAP user name includes an invalid character:

12a Manually add the user with a user name that is valid in GroupWise.

See "Manually Creating GroupWise Accounts" on page 454.

12b Manually associate the GroupWise user with the LDAP user.

See "Associating GroupWise Users with an LDAP Directory" on page 467.

13 (Conditional) If you have imported users from an LDAP directory other than NetIQ eDirectory, and if you use GroupWise Messenger with your GroupWise system, see "Messenger" in the *GroupWise 18 Interoperability Guide*.

14 Skip to "Configuring New GroupWise Accounts" on page 455.

Manually Creating GroupWise Accounts

If you have users who do not have accounts in your LDAP directory, you can still assign them GroupWise accounts.

1 In the GroupWise Admin console, click **Users**, then click **New**.

2 Fill in the following fields:

User Name: Specify the user's GroupWise user name. The user name, along with the user's Internet domain name, provide the user with a unique email address. Do not use any of the characters listed in "Invalid Characters in GroupWise Object Names and Email Addresses".

IMPORTANT: Characters that are valid and even desirable in a GroupWise user name, such as accented characters, might not be valid in an email address. For some users, you might need to set up a preferred email ID in order to ensure that they have a valid email address. For instructions, see "Setting a Preferred Email ID" on page 279.

First Name: Specify the user's first name or given name.

Last Name: Specify the user's last name or surname.

Post Office: Select the post office where you want the user's mailbox.

3 Click **OK** to create the new GroupWise user.

The user is given a GroupWise mailbox in the post office you selected and can access his or her mailbox through the GroupWise client or GroupWise WebAccess.

4 (Conditional) If you use GroupWise Messenger with your GroupWise system, see "Messenger" in the *GroupWise 18 Interoperability Guide*.

5 Continue with Configuring New GroupWise Accounts.

Configuring New GroupWise Accounts

1 In the GroupWise Admin console, browse to and click the name of a new user.

2 (Optional) Modify any of the following fields on the **Account** tab:

File ID: This three-letter ID is randomly generated and is non-editable. It is used for various internal purposes within the GroupWise system, including ensuring that files associated with the user have unique names.

Restore Area: This field applies only if you are using the GroupWise backup and restore features. If so, this field indicates the location where the user's mailbox is being backed up. For details, see Chapter 49, "Restoring GroupWise Databases from Backup," on page 423.

Visibility: Select the level at which you want the user to be visible in the GroupWise Address Book. For more information, see "Controlling Object Visibility" on page 72.

External Sync Override: This option applies only if your GroupWise system links to and synchronizes with an external system. For more information, see "Using an External Domain to Connect GroupWise Systems" on page 112.

- **Synchronize According to Visibility:** The user information is synchronized to external systems only if visibility is set to **System**.
- **Synchronize Regardless of Visibility:** The user information is synchronized to external systems regardless of the object visibility.
- **Don't Synchronize Regardless of Visibility** The user information is not synchronized to external systems.

LDAP Authentication: (Conditional) If you need to override the user name for authenticating to the LDAP server, specify the user's LDAP DN in the format used by your LDAP server. For example:

```
cn=user_name,ou=org_unit,o=organization
cn=user_name,ou=users,dc=server_name,dc=company_name,dc=com
```

LDAP Authentication Directory: (Conditional) After you specify the user's LDAP DN, select the LDAP directory where the user is located.

Expiration Date: If you want the user's GroupWise account to no longer work after a certain date, specify the expiration date. For more information, see "Expiring a GroupWise Account" on page 475.

Disable Logins: Select this option to prevent the user from accessing his or her GroupWise mailbox. For more information, see "Disabling and Enabling GroupWise Accounts" on page 473.

3 (Conditional) If the user was imported from an LDAP directory, click the **General** tab to see the user information that has been imported from the LDAP directory.

When user information changes in the LDAP directory, it is automatically synchronized to GroupWise.

4 (Conditional) If the user was manually created, click the **General** tab to provide user information.

5 (Optional) Click the **Internet Addressing** tab to customize the user's email address information.

For more information, see "Overriding Internet Addressing" on page 278.

6 (Optional) Click the **Objects** tab to configure how the new user associates with other GroupWise objects:

7 Click **Save**, then click **Close** to return to the main Admin console window.

Adding User Photos to the System Address Book

User photos can be added to the System Address Book. When they are added, they can be viewed in address books, when selecting user through name completion, in the header when viewing items that you have received, and other places where you can view users. Photos can be added through the admin console in the following ways:

- **During user import from LDAP:** In the **Admin Console** > **System** > **User Import**, if you select **Import User Photo** and the user has a photo associated with their LDAP account, the photo will be imported and used in GroupWise.
- **Associating a GroupWise user to an LDAP object:** If you have a user that was created in GroupWise and associate them to an LDAP user that has a photo connected to their LDAP account, it will associate that photo with the GroupWise user. This is done through the **Admin Console** > **Users** > *(select a specific user)* > **More** > **Associate**.
- **Adding the image through the user's properties page:** In the user's properties page, you can click the Edit option that appear when you hover over the image in the top left of the page to edit the user's photo. The user's properties page is found in the **Admin Console** > **Users** > *(select a specific user)*.

NOTE: When you upload photos to the System Address Book, they are automatically sized to 64 pixels x 64 pixels by GroupWise, so the size of the original photo does not matter. You may want to make sure that the photo sizes properly to this size before uploading.

If you would like users to be able to add or edit their own photos, you can enable this functionality in their client:

1. Go to the **Admin Console** > *(select domain or post office)* > **Client Options** > **Environment** > **Address Book**.
2. Select **Allow update of picture in the System Address Book**.
3. Click **OK**.

This will allow users to change their photo that is displayed in the System Address Book. If a user updates their photo, it is only stored in GroupWise and does not sync back to a directory.

Educating Your New Users

After users can log in to their GroupWise accounts, all of the GroupWise clients features are at their fingertips, but some new users do not know how to get started. You can give your users the following suggestions to encourage them to explore GroupWise:

You can also provide users with **Quick Starts** that cover specialized GroupWise functionality:

- *Calendar Publishing Quick Start*
- *GroupWise and Skype Quick Start*
- *GroupWise and Messenger Quick Start*
- *GroupWise and Vibe Quick Start*
- *WebAccess Basic Interface Quick Start* for mobile device users

You can also refer users to the GroupWise 18 User Frequently Asked Questions.

NOTE: For convenience in printing, all GroupWise User Guides are available in PDF format at the GroupWise 18 Documentation website (http://www.novell.com/documentation/groupwise18/).

GroupWise Client

In the GroupWise client:

- Click **Help** > **Help Topics** to learn to perform common GroupWise tasks.
- Click **Help** > **What's New** to learn about the latest new GroupWise features.
- Click **Help > Training and Tutorials** to display the BrainStorm, Inc. QuickHelp for GroupWise 18 (http://www.brainstorminc.com/videos/gw18) or customized training materials provided for your users.

  You can change the URL that displays when users click **Help > Training and Tutorials**. In the GroupWise Admin console, use **Client Options > Integration > Tutorial** on a domain, post office, or user to specify the URL for your customized training materials.
- Click **Help** > **User Guide** to view the *GroupWise 18 Client User Guide* in HTML format. The guide includes more background information on GroupWise features than the Help does.

GroupWise WebAccess

In GroupWise WebAccess:

- Click **Options > Help** to learn to perform common WebAccess tasks.
- Click **Options > Help** > **What's New in GroupWise 18 WebAccess** to learn about the latest new WebAccess features.
- Click **Options > Help** > **Micro Focus GroupWise 18 Documentation Website** to access the *GroupWise 18 WebAccess Mobile User Guide*. The guide includes more background information on GroupWise features than the Help does.

GroupWise WebAccess Mobile

In GroupWise WebAccess Mobile:

- Click **Options > Help** to learn to perform common WebAccess tasks on your tablet.
- Click **Options > Help** > **What's New in GroupWise 18 WebAccess Mobile** to learn about the latest new WebAccess features for your tablet.
- Click **Options > Help** > **Micro Focus GroupWise 18 Documentation website** to access the *GroupWise 18 WebAccess User Guide*. The guide includes more background information on GroupWise features than the Help does.

53 Managing GroupWise Accounts and Users

As your GroupWise system grows, you will need to add users and manage their GroupWise accounts.

See also:

- Chapter 42, "Maintaining Domain and Post Office Databases," on page 395
- Chapter 43, "Maintaining User/Resource and Message Databases," on page 403
- Chapter 48, "Backing Up GroupWise Databases," on page 421

Proper database maintenance and backups allow recovery from accidental deletions, as described in the following sections:

- "Restoring Deleted Mailbox Items" on page 425
- "Recovering Deleted GroupWise Accounts" on page 428

Adding a User to a Group

GroupWise groups are sets of users and resources that can be addressed as a single entity. When a GroupWise user addresses an item (message, appointment, task, or note) to a group, each user or resource that is a member receives a copy of the item.

1. In the GroupWise Admin console, browse to and click the name of user.
2. Click the **Objects** tab, then click **Groups**.
3. Click **Add**, select one or more groups that you want to add the user to, then click **OK**.

   By default, the user is added as a primary recipient (**To** recipient).
4. (Optional) If you want to change the user's recipient type, select the group, click **Participation**, then click **To**, **CC**, or **BC**.
5. Click **Save**, then click **Close** to return to the main Admin console window.

Allowing Users to Modify Groups

Because groups are created in the GroupWise Admin console, users by default cannot modify them. However, in the GroupWise Admin console, you can grant rights to selected users to modify specific groups. For setup instructions, see "Enabling Users to Modify a Group" on page 488.

Adding a Global Signature to Users' Messages

You can build a list of globally available signatures to be automatically appended to messages sent by GroupWise client users. Global signatures are created in HTML format. For users who prefer the Plain Text compose view in the GroupWise client, a plain text version of the signature is appended instead of the HTML version. When this occurs, HTML formatting and embedded images are lost, but you can customize the plain text version as needed to compensate for the loss of HTML formatting.

The global signature is appended by the GroupWise client to messages after any personal signatures that users create for themselves. It is appended after the user clicks **Send**. If S/MIME encryption is enabled, the global signature is encrypted along with the rest of the message. GroupWise client users can choose whether global signatures are appended only for recipients outside the local GroupWise system or for all recipients, local as well as external. For GroupWise client users, you can assign a global signature based on users, resources, post offices, and domains.

The Internet Agent (GWIA) can append global signatures to the end of messages for recipients outside the local GroupWise system. However, the GWIA does not append global signatures to S/MIME-encoded messages, nor does it duplicate global signatures already appended by the GroupWise client. You can assign a default global signature for all users in your system, and then override that default by editing the properties of each GWIA object

---

NOTE: If a user sends an external message with a subject only (no message body), a global signature is not appended. This is working as designed. The presence of a global signature on an external message with an empty message body would prevent the GWIA /flatfwd switch from functioning correctly.

Creating Global Signatures

1. In the GroupWise Admin console, click **System** > **Global Signatures**.
2. Click **New** to create a new global signature.
3. Specify a descriptive name for the signature.
4. Compose the signature using the basic HTML editing tools provided, then click **OK** to add the new signature to the list in the Global Signatures dialog box.
5. (Conditional) If you want to check or edit the text version of the signature that was automatically generated:
   - **5a** Click the name of the new signature
   - **5b** Modify the text version of the signature as needed, then click **OK**.
6. Click **Close** in the Global Signatures dialog box to save the list.

Setting a Default Global Signature

1. In the GroupWise Admin console, click **System > Global Signatures**.
2. In the list of global signatures, select the global signature that is appropriate for most GroupWise users, then click **Set Default**.
3. Click **Close**.

Assigning Global Signatures to GWIAs

When your organization needs more than one global signature on outgoing messages, you can assign different global signatures to GWIAs as needed.

1. In the GroupWise Admin console, browse to and click the GWIA.
2. Click the **SMTP/MIME** tab, then click **Message Formatting**.
3. Under **Default Global Signature to Insert in Outbound Messages**, select **Override**, then select the global signature that you want this GWIA to append to messages.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Assigning Global Signatures to GroupWise Client Users

For GroupWise client users, you can assign different global signatures to different sets of users by domain, post office, and individual user.

A global signature set at the post office level overrides the global signature set at the domain level. A global signature set at the user level overrides the global signature set at the post office and domain level.

1. In the GroupWise Admin console, browse to and select the domain, post office, or set of users to which you want to assign a global signature.
2. Click **Client Options**.
3. Click the **Send** tab, then click **Global Signature**.
4. In the **Global Signature** drop-down list, select the global signature that you want to use.

   By default, the selected signature is applied only to messages that are being sent outside your GroupWise system.
5. (Optional) If you want to also use global signatures internally, select **Apply Signature to All Messages**.
6. Click **OK** to save the settings.

Excluding Global Signatures

You might have a domain, post office, or set of users where you do not want the global signature to be added to messages. You can suppress global signatures at the domain, post office, or user level.

1. In the GroupWise Admin console, browse to and select the domain, post office, or users for which you want to suppress a global signature.
2. Click **Client Options**.
3. Click the **Send** tab, then click **Global Signature**.
4. In the **Global Signature** drop-down list, select **<None>**, then click **OK**.

Moving GroupWise Accounts

Expansion or consolidation of your GroupWise system can make it necessary for you to move GroupWise accounts from one post office to another. When you move a GroupWise account, the user's mailbox is physically moved from one post office directory to another.

When you move a user's GroupWise account, all items are moved correctly and all associations (proxy rights, shared folder access, and so on) are resolved so that the move is transparent to the user. Occasionally, some client options the user has set (GroupWise client > **Tools** > **Options**) might be lost and must be re-created for the new mailbox.

The following sections provide information you should know before performing a move and instructions to help you perform the move.

Live Move vs. File Transfer Move

GroupWise provides two types of moves: a live move and a file transfer move.

A live move uses a TCP/IP connection between POAs to move a user from one post office to another. In general, a live move is significantly faster (approximately 5 to 10 times) than a file transfer move. However, it does require that TCP/IP is functioning efficiently between the two POAs.

A file transfer move uses the transfer of message files (using POAs and MTAs) rather than a TCP/IP connection between POAs. A file transfer move is required if you are moving a user across a WAN link where TCP/IP might not be efficient.

By default, when you initiate a user move, the post office's POA attempts to establish a live move session with the destination post office's POA. If it cannot, a file transfer move is used instead.

If desired, you can disable the live move capability (Post Office object > **GroupWise** > **Settings > Disable Live Move**). Any moves to or from the post office would be done by file transfer.

Preparing for a User Move

Proper preparation can make the process of moving users go more smoothly. Consider the following before moving a user's GroupWise account:

- Ensure that the POAs for the user's current post office and destination post office are running.

  See Chapter 17, "Monitoring the POA," on page 163.
- Configure both POAs for verbose logging, in case troubleshooting is required during the user move process.

  See "Using POA Log Files" on page 166.
- If you are performing the user move during off hours, optimize both POAs for the user move process. On the **Agent Settings** tab of the POA object in the GroupWise Admin console, set **Max Thread Usage for Priming and Moves** to 80%. Set **Client/Server Handler Threads** to 40.

  See "Optimizing Client/Server Processing" on page 171.
- Ensure that the MTA for the user's current domain and destination domain (if different) are running.

  See Chapter 24, "Monitoring the MTA," on page 237.
- Ensure that all links between POAs and MTAs are open.

  See "Using the Link Configuration Tool" on page 106, "Link Trace Report" on page 657, and "Link Configuration Report" on page 657.

- Ensure that all domain databases along the route for the user move are valid.

  See “Validating Domain or Post Office Databases” on page 395.
- Ensure that the mailbox to move is valid. Select the **Structure**, **Index**, and **Contents** options in GroupWise Check (GWCheck) or in Mailbox/Library Maintenance in the GroupWise Admin console.

  See “Analyzing and Fixing User/Resource and Message Databases” on page 403.
- Enable automatic creation of nicknames for moved users, so that replies and forwarded messages can be delivered successfully after the user has been moved.

  See Chapter 61, “Configuring Automatic Nickname Creation,” on page 507.
- A user who owns a resource cannot be moved. If the user owns a resource, reassign ownership of the resource to another user who is on the same post office as the resource. You can do this beforehand, or when initiating the user move.

  See “Changing a Resource’s Owner” on page 498
- (Optional) To reduce the number of mailbox items that must be moved, ask the user to clean up his or her mailbox by deleting or archiving items. Have the user empty the Trash so that deleted items are not moved with the user.
- (Optional) Have the user exit the GroupWise client and GroupWise Notify before you initiate the move. When the move is initiated, the user’s POA first creates an inventory list of all information in the user’s mailbox. This inventory list is sent to the new post office’s POA so that it can verify when all items have been received. If the user has not exited when the move begins, the user is automatically logged out so that the inventory list can be built. However, after the move has been initiated, the user can log in to his or her new mailbox even if the move is not complete.

Moving a GroupWise Account to Another Post Office

1. In the GroupWise Admin console, click **Users**.
2. Select the users you want to move, then click **Move**.
3. Select the post office to which you want to move the user’s account.
4. (Optional) Select **Create Nickname(s) for the Selected Object(s)**, so that messages that will be undeliverable to the old email address are successfully delivered to the new email address.

   For more information, see Part XII, “Nicknames,” on page 501.
5. Click **OK** to initiate the user move.
6. (Conditional) If necessary, select a new owner for the resource, then click **OK**.
7. Keep track of the user move process using the User Move utility.

   See “Monitoring User Move Status” on page 464.

Resolving Addressing Issues Caused By Moving an Account

The user’s new address information is immediately replicated to each post office throughout your system so that the GroupWise Address Book contains the user’s updated address. Any user who selects the modified user from the GroupWise Address Book can successfully send messages to the user.

However, some users might have the user’s old email address in their Frequent Contacts address book. In this case, if the sender types the modified user’s name in the **To** field rather than selecting it from the Address Book, GroupWise uses the old email address stored in the Frequent Contacts address book instead of the new email address in the GroupWise Address Book. This results in the message being undeliverable.

The POA automatically resolves this issue when it performs its nightly user upkeep. During the nightly user upkeep process, the POA ensures that all addresses in a user's Frequent Contacts address book are valid addresses in the GroupWise Address Book. For more information, see "Configuring Nightly User Upkeep" on page 157.

If you want to ensure that messages sent to the user's old email address are delivered even before the POA cleans up the Frequent Contacts address book, you can create a nickname using the old GroupWise email address. For more information, see Part XII, "Nicknames," on page 501.

Monitoring User Move Status

The User Move Status tool helps you track progress as you move users and resources from one post office to another. You can display all of the user moves in your GroupWise system. Or you can display the user moves associated with the object that you selected before displaying the User Move Status tool. For example, if you selected a Domain object, all user moves for the selected domain are displayed, but not user moves for other domains.

While a GroupWise user account is being moved, the POA in the source post office and the POA in the destination post office communicate back and forth. You can track the move process progresses through various steps and statuses:

1. In the GroupWise Admin console, browse to and click the name of a post office or domain, click the **Objects** tab, then click **User Move Status** to display the user moves specific to the post office or domain.

   or

   Click **System > User Move Status** to display all users moves in your GroupWise system.

   All moves occurring within the selected location are listed.

   At the beginning of the move process, most buttons are dim, because it would not be safe for you to perform those actions at that point in the move process. When those actions are safe, the buttons become active.
2. (Optional) To restrict the number of users and resources in the list, type distinguishing information in any of the **Search** field, then press Enter to filter the list.
3. During the move, click **Refresh** to update the status information.

   IMPORTANT: The list does not refresh automatically.

   During the move, you might observe some of the following statuses:

   - **Destination post office updated:** The destination POA has updated the destination post office database with the user's account information. At this point, the user account exists in the new location and appears in the GroupWise Address Book with the new location information.
   - **Source post office updated:** The source POA has updated the user in the source post office database to show the new destination post office. At this point, the user can no longer access the mailbox at the old location.
   - **Moving mailbox information:** The POAs have finished exchanging administrative information and are ready to move items from the old mailbox to the new mailbox.
   - **Sending mailbox inventory list:** The source POA sends the destination POA a list of all the mailbox items that it should expect to receive.
   - **Send item request:** The destination POA starts requesting items from the source POA and the source POA responds to the requests

- **Retry mailbox item retrieval:** The destination POA was unable to retrieve an item and is retrying. The POA continues to retry every 12 hours for 7 days, then considers the move complete. To complete the move without waiting, click **Force Complete**. Typically, items that cannot be moved were not accessible to the user in the first place, so nothing is missed in the destination mailbox.
- **Completed retrieving items:** The destination POA has received all of the items on its mailbox inventory list.
- **Move completed:** After all of the user's mailbox items have arrived in the destination post office, the user's original account in the source post office is deleted and the user move is finished.

4 If something disrupts the user move process, select the problem user or resource, then click **Retry/Restart**.

5 Select the option appropriate to the problem you are having, then click **OK**.

Retry the Last Step of the Mailbox Move: Select this option to retry whatever step the user move process has stopped on. This is equivalent to performing one of the POA's automatic retries manually and immediately. Ideally, the step completes successfully on the retry and processing continues normally.

Skip Retry on the Current Mailbox Item: Select this option to skip a particular mailbox item that cannot be successfully moved. The need for this action can usually be avoided by running Mailbox/Library Maintenance on the mailbox before moving the user account. Ideally, the user move processing should continue normally after skipping the problem item.

Stop Deferred Retries: Select this option to stop the POA from retrying to send items that have not been successfully received. This completes the user move process even though some individual items have not been moved successfully.

Restart the Entire Mailbox Move: Select this option if something major disrupts the user move process and you want to start over from the beginning. Because nothing is deleted from the source mailbox until everything has been received in the destination mailbox, you can safely restart a move at any time for any reason.

After you have moved a user in the GroupWise Admin console, you can display detailed information about items belonging to that account that have not yet been moved to the destination post office, perhaps because problems were encountered when trying to move them. This information can help determine the importance of moving residual items that are still pending after all other items have been successfully moved.

6 Assess the importance of items that are still pending.

6a Select an account for which the move has not completed, then click **Pending Items**.

You can determine the record type (item, folder, GroupWise Address Book contact, and so on), the item type (mail, appointment, task, and so on), how old the item is, the sender of the item, and the **Subject** line of the item. Not all columns in the Pending Items dialog box apply to all record types and item types, so some columns might be empty.

6b Click **Request** to request pending items.

Pending items are retrieved in groups of 25.

6c Click **Yes** to request the first group of pending items, then click **OK**.

You might need to wait for a while before the pending item lists displays because the request goes out through the destination domain to the source domain to the source post office, where the source POA sends the requested information back to the destination domain. Do not click **Request** again before the list appears or you receive the same list twice.

When the pending items appear, you can select an item, then click **Info** to display detailed information about the item. You can also click **Refresh** to reread the domain database to determine if additional items have been moved.

6d If you and the user whose mailbox is being moved decide that the pending items are expendable, click **Force Complete** to finish the move process.

Renaming Users and Their GroupWise Accounts

When you rename a user, all of the user's associations remain unchanged. For example, the user retains ownership of any resources and documents while other users who had proxy rights to the user's mailbox retain proxy rights.

1. Ensure that the user has exited the GroupWise client and GroupWise Notify.
2. Ensure that the domain's MTA and post office's POA are running.
3. In the GroupWise Admin console, browse to and click the name of a user, then click **More > Rename**.
4. Specify the new GroupWise user name.
5. (Optional) Select **Create Nickname for This User** so that messages that will be undeliverable at the old email address are successfully delivered to the new email address.

   For more information, see Part XII, "Nicknames," on page 501.
6. Click **OK** to rename the user.

Resolving Addressing Issues Caused By Renaming a User

The user's new address information is immediately replicated to each post office throughout your system so that the GroupWise Address Book contains the user's updated address. Any user who selects the modified user from the GroupWise Address Book can successfully send messages to the user.

However, some users might have the user's old email address in their Frequent Contacts address book. In this case, if the sender types the modified user's name in the **To** field rather than selecting it from the Address Book, GroupWise uses the old email address stored in the Frequent Contacts address book instead of the new email address in the GroupWise Address Book. This results in the message being undeliverable.

The POA automatically resolves this issue when it performs its nightly user upkeep. During the nightly user upkeep process, the POA ensures that all addresses in a user's Frequent Contacts address book are valid addresses in the GroupWise Address Book. For more information, see "Configuring Nightly User Upkeep" on page 157.

If you want to ensure that messages sent to the user's old email address are delivered even before the POA cleans up the Frequent Contacts address book, you can create a nickname using the old GroupWise email address. For more information, see Part XII, "Nicknames," on page 501.

Changing the LDAP Directory Association of Users

If you set up a new GroupWise system by manually creating GroupWise users in the GroupWise Admin console, you can later associate those GroupWise users with users in an LDAP directory. The directory then becomes the primary location for user information. User synchronization updates the user information in GroupWise based on the information in the LDAP directory. It can also publish users' email addresses to the LDAP directory.

Associating GroupWise Users with an LDAP Directory

1. In the GroupWise Admin console, configure your GroupWise system to communicate with the LDAP directory.

   For instructions, see "Setting Up an LDAP Directory" on page 79.
2. Click **System > Directory Associations**.
3. (Conditional) If you have multiple LDAP directories, select the one where you want to associated the GroupWise users.
4. (Conditional) If the context of the User objects is under the Base DN, browse to and select the LDAP context where User objects are located.
5. (Optional) Specify an LDAP filter and select additional options as needed.
6. Click **Preview** to list the users who will be associated with LDAP directory objects.
7. (Conditional) As needed, adjust the filter and options, then click **Update Preview** until you are satisfied with the list.
8. When you are satisfied with the list, click **Associate**.

   The GroupWise users are associated with their LDAP directory counterparts.

Migrating From eDirectory to Active Directory

The process of migrating from NetIQ eDirectory to Microsoft Active Directory is straightforward. Before you start the migration, ensure that both directories are stable.

- "Preparing for the Migration" on page 467
- "Creating the Directory Associations" on page 468
- "Verifying the Directory Associations" on page 468
- "Verifying Successful Authentication" on page 469
- "Verifying a Complete User Migration" on page 469

Preparing for the Migration

The Active Directory object in your GroupWise system must be properly configured to support the migration process.

1. In the GroupWise Admin console, click **System > LDAP Servers**.
2. Click the name of the Active Directory object.
3. Verify that the **Base DN** field displays the location where you plan to create the Active Directory User objects for the GroupWise users. Update it if necessary.
4. Verify that the **Sync Domain** field displays the domain where the users' post office and GroupWise mailboxes are located.
5. Verify that **Enable Synchronization** is selected.
6. On the **Email Publishing** tab, verify that **Publish Email Addresses to This Directory** is selected.
7. Click **OK**, then click **Close**.
8. Continue with Creating the Directory Associations.

Creating the Directory Associations

1. Create a User object in Active Directory for each GroupWise user.

   IMPORTANT: Ensure that, on each new Active Directory User object, the **User logon name (pre-Windows 2000)** field (the sAMAccountName property in Active Directory) exactly matches the GroupWise user name (the uniqueID property in eDirectory). Any user for whom these names do not match must be manually migrated.

   ---

2. In the GroupWise Admin console, click **System > Directory Associations**.
3. Select the LDAP directory that you verified in “Preparing for the Migration” on page 467.
4. (Conditional) If the context of the User objects is under the Base DN, browse to and select the LDAP context where User objects are located.
5. Select **Override Existing Association**.

   By default, existing users retain their existing associations. The migration process requires that eDirectory associations be replaced with Active Directory associations.
6. (Optional) Specify an LDAP filter and select additional options as needed.
7. Click **Preview** to list the users who will be migrated from eDirectory to Active Directory.
8. (Conditional) As needed, adjust the filter and options, then click **Update Preview** until you are satisfied with the list.

   TIP: Initially, migrate only a small number of users to ensure that the migration process is working as expected.

   ---

9. Click **Associate**.
10. Continue with Verifying the Directory Associations.

Verifying the Directory Associations

When the associations between GroupWise and Active Directory are properly set up, GroupWise data synchronizes reliably between the two systems.

1. In Active Directory, verify that the user’s GroupWise information has synchronized to Active Directory:
   - **1a** On the **General** tab of a GroupWise User object, verify that the **Email Address** field displays the user’s GroupWise email address.
   - **1b** To provide a test of user synchronization from Active Directory to GroupWise, modify the user’s phone number.
2. In the GroupWise Admin console, ensure that the MTA console is password protected so that you can control the MTA in your web browser:
   - **2a** Browse to and click the MTA that synchronizes GroupWise data with Active Directory.
   - **2b** Click the **Agent Settings** tab, then verify that the **HTTP** section shows that the MTA is configured with an HTTP user name and password.
   - **2c** (Conditional) If necessary, provide a user name and password.
   - **2d** Click **Save**, then click **Close** to return to the main Admin console window.

3 In the MTA console, perform user synchronization between GroupWise and Active Directory:

3a When prompted, provide the user name and password that are required for controlling the MTA in the MTA console.

3b On the **Configuration** tab, click **Directory User Synchronization**.

3c Select **Perform GroupWise Directory Synchronization Now**, then click **Submit**.

3d Click the **Log Files** tab, then view the most recent log file to look for lines similar to the follow example:

```
12:35:56 0378 Synchronizing Directory Example Active Directory
12:35:56 0378 Connecting to LDAP server at 192.168.1.255 for Directory Example Active Directory
12:35:57 0378 Checking Provo2.Marketing.fdriscoll
12:35:57 0378 Checking Provo2.Marketing.nopdyke
12:35:57 0378 Checking Provo2.Marketing.rbranagan
12:35:57 0378 Disconnecting from LDAP server for Directory Example Active Directory
12:35:57 0378 Synchronization complete for Directory Example Active Directory
12:35:57 0378 Disconnecting from LDAP server for Domain Provo2
```

4 In the GroupWise Admin console, verify that the user's information in Active Directory has synchronized to GroupWise:

4a Click **Users**, then click the name of the user whose phone number you modified in Active Directory in Step 1b.

4b On the **General** tab, verify that the user's phone number matches what is in Active Directory.

4c Change the user's phone number back, then click **Save**.

5 Continue with Verifying Successful Authentication.

Verifying Successful Authentication

When the associations are correctly set up, GroupWise users can log in to their mailboxes by using LDAP authentication.

1 In the GroupWise Admin console, verify that the post office of the migrated users is configured for LDAP authentication:

1a Browse to and click the name of the post office.

1b On the **Security** tab, verify that **LDAP Authentication** is selected.

2 Start the GroupWise client for a user that has been migrated to Active Directory.

3 Verify that the user credentials provided by Active Directory result in a successful login into the GroupWise mailbox.

4 Continue with Verifying a Complete User Migration.

Verifying a Complete User Migration

After you have used the Directory Associations tool to migrate all of your users from eDirectory to Active Directory, you can verify that, in fact, no more users remain in eDirectory.

1 In the GroupWise Admin console, click **Users** to list all of your GroupWise users.

2 Use the **Search User Name** field to check for users that might have been missed:

2a Use the following filter to search for users who are not currently associated with any LDAP directory:

```
directory = null
```

2b Use the following filter to search for users who are not associated with Active Directory:

directory != *active_directory_name*

3 (Conditional) If your searches revealed orphan users that no longer need GroupWise accounts, plan to disable their accounts at an appropriate time.

For instructions, see "Disabling and Enabling GroupWise Accounts" on page 473.

4 (Conditional) If your searches revealed users whose Active Directory logon name did not match their GroupWise user name, you can associate them manually:

4a After searching for the unassociated users, click a user name.

4b Click **More > Associate**.

4c Select the LDAP directory where you want to associate the user.

4d Browse to and select the user in the LDAP directory.

4e Click **OK**.

When you are sure that you no longer need the User objects in eDirectory, you can delete them.

Using an SSL connection between GroupWise and Active Directory is strongly recommended. The process for establishing an SSL connection is beyond the scope of the GroupWise product documentation.

Dissociating GroupWise Users from an LDAP Directory

1 In the GroupWise Admin console, browse to and click the name of the User that you want to dissociate from the LDAP directory.

2 Click **More > Dissociate**.

3 Verify that the right user information is displayed, then click **OK**.

The user is still a GroupWise user, but the user is no longer associated with a User object in an LDAP directory.

Managing Mailbox Passwords

The following sections provide information to help you manage GroupWise mailbox passwords:

- "Creating or Changing a Mailbox Password" on page 470
- "Removing a Mailbox Password" on page 471

For more information about GroupWise passwords, see Chapter 89, "GroupWise Passwords," on page 687.

Creating or Changing a Mailbox Password

If a user can log in to GroupWise, he or she can also change the mailbox password through the Security Options dialog box in the GroupWise client (**Tools** > **Options** > **Security**) or on the Passwords page in GroupWise WebAccess (**Options** > **Password**).

As administrator, you can use the GroupWise Admin console to create or change a password for a user.

1 In the GroupWise Admin console, browse to and click the name of the user.

2 Click **Change Password**.

3 Specify and confirm the password.
4 Click **OK**.

Removing a Mailbox Password

If you want to remove a user's mailbox password but not assign a new password, you can clear the password.

1 In the GroupWise Admin console, browse to and click the name of the user.
2 Click **Change Password**.
3 Select **Clear User's Set Password**.
4 Click **OK**.

NOTE: A mailbox with no password cannot be accessed using GroupWise WebAccess.

Managing User Email Addresses

To ensure that user addresses meet your needs, GroupWise enables you to determine the format and visibility of addresses, as well as create additional names for users.

Ensuring Unique Email Addresses

You can use the same user name for more than one user in your GroupWise system, if each user is in a different Internet domain. Rather than requiring that each user name be unique in your GroupWise system, each combination of user name and Internet domain must be unique. This provides more flexibility for handling the situation where two people have the same name.

When adding or changing users' email addresses you can check to ensure that the email address you want to use for a particular user is not already in use.

1 In the GroupWise Admin console, click **System** > **Email Address Lookup**.
2 In the **Search** field, specify the email address.

   You can specify the user name only (for example, `jsmith`) or the entire address (for example, `jsmith@novell.com`).
3 Press Enter.

   All objects whose email address match the one you specified are displayed.
4 (Optional) Click the object ID to see details about the object.

Publishing Email Addresses to Your LDAP Directory

If you are planning to import users from your LDAP directory into your GroupWise system, you can publish the GroupWise email addresses back to your LDAP directory.

1 Ensure that LDAP user synchronization is enabled.

   For setup instructions, see "Configuring User Synchronization for an LDAP Directory" on page 80.
2 In the GroupWise Admin console, click **System > LDAP Servers**.

3 In the list of LDAP servers and directories, click the name of the LDAP directory, then click the **Email Publishing** tab.

4 Select **Publish Email Addresses to This Directory**, then select the types and formats of addresses that you want to publish.

For background information, see "Understanding Internet Addressing Formats" on page 274.

5 Click **OK**.

If your users are associated with User objects in an LDAP directory, and if you changed the preferred address format, you are prompted to update the email addresses for the affected users in the LDAP directory. We recommend that you allow this update. However, performing it for a large segment of your GroupWise system might take a while.

LDAP user synchronization publishes the email addresses to your LDAP directory when they change in GroupWise.

6 Click **Yes** to confirm, then click **Close** when the process is completed.

Changing a User's Internet Addressing Settings

By default, a user inherits the Internet address settings (preferred Internet address format, allowed address formats, and Internet domain name) from the user's post office, domain, or GroupWise system. If necessary, you can override these settings for a user. For more information, see "Overriding Internet Addressing" on page 278.

Changing a User's Visibility in the Address Book

A user's visibility level determines the extent to which the user's address is visible throughout your GroupWise system. You can make the user visible in the Address Book throughout your entire GroupWise system, you can limit visibility to the user's domain or post office only, or you can make it so that no users can see the user in the Address Book. For instructions, see "Controlling Object Visibility" on page 72.

Synchronizing User Information

When you associate GroupWise users with LDAP users (such as users in NetIQ eDirectory or Microsoft Active Directory), the MTA handles automatic synchronization of user information from the LDAP directory to GroupWise on a regular schedule. For background information, see "Configuring User Synchronization for an LDAP Directory" on page 80.

You can manually perform the user synchronization if information has changed in the LDAP directory, and you want to see it immediately in GroupWise.

1 In the GroupWise Admin console, browse to and click the name of a user.

2 Click **Synchronize**.

Disabling and Enabling GroupWise Accounts

You can disable a GroupWise account so that the user cannot access his or her mailbox until you enable the account again. This might be necessary when a user leaves the company and no longer needs access to the mailbox.

1. In the GroupWise Admin console, browse to and click the name of a user.
2. Click the **Accounts** tab, then select **Disable Logins**.
3. Click **Save**, then click **Close** to return to the main Admin console window.
4. (Conditional) If the user is logged in to his or her Online mailbox when you disable logins, disconnect the user.

   For instructions, see "Disconnecting a User Session from the POA" on page 161.
5. To enable the user's account when access is again permitted, deselect **Disable Logins**, click **Save**, then click **Close**.

While a user's account is disabled, other users to whom proxy rights have been granted can still access the mailbox. This is convenient for reviewing the contents of the mailbox of a departed employee and pulling out those messages that are of use to the incoming employee.

Unlocking GroupWise Accounts

A GroupWise user's account is automatically disabled (locked) if you have enabled intruder detection, and if the user exceeds the number of unsuccessful login attempts that you have allowed. For more information, see "Configuring Intruder Detection" on page 153.

When a user is locked out, access is automatically granted again after the incorrect login reset time interval has passed. If a user needs quicker access, you can unlock the GroupWise account in the GroupWise Admin console or in the POA console.

In the GroupWise Admin console:

1. In the GroupWise Admin console, browse to and click the name of a user.
2. Click the **Accounts** tab, then deselect **Disable Logins**.
3. Click **Save**, then click **Close** to return to the main Admin console window.

In the POA console:

1. Click **Status**.
2. In the **Statistics** section, click **Intruder Detection**.
3. Click the user name of the locked out user.
4. Select **Reset Lockout**, then click **Submit**.

As soon as the POA receives the changed setting, the user can again log in.

Checking GroupWise Account Usage

You can identify GroupWise accounts that have been inactive for a specified period of time. See "Auditing Mailbox License Usage in the Post Office" on page 127.

You can measure message traffic from individual GroupWise mailboxes. See "User Traffic Report" on page 662.

Forcing Inactive Status

If you have a GroupWise mailbox that contains information of lasting value, but that does not have an current user associated with it, you can force the mailbox into inactive status to lessen the ongoing licensing costs for the mailbox.

1 In the GroupWise Admin console, browse to and click the name of a user.
2 Click the **Accounts** tab, then select **Force Inactive Status**.
3 Click **Save**, then click **Close** to return to the main Admin console window.

For complete information about licensing, see "Auditing Mailbox License Usage in the Post Office" on page 127.

Removing GroupWise Accounts

You can remove a user's GroupWise account by deleting or expiring it. Deleting an account removes the entire account (address, mailbox, items, and so on) from the GroupWise system. Expiring an account deactivates the account so that it cannot be accessed, but does not remove it from the system. The following sections provide information to help you delete or expire GroupWise accounts

- "Deleting a GroupWise Account" on page 474
- "Expiring a GroupWise Account" on page 475
- "Managing Expired or Expiring GroupWise Accounts" on page 475

If you delete a GroupWise account by accident, or need to retrieve a deleted account for some other reason, see "Recovering Deleted GroupWise Accounts" on page 428.

NOTE: When you remove a GroupWise account, any personal databases, such as an archive, a Caching mailbox, or a Remote mailbox, that are associated with the account are unaffected by the account deletion. Such databases are not located where the GroupWise Admin console could delete them, so they must be deleted manually.

Deleting a GroupWise Account

When you delete a user's GroupWise account, the user's mailbox is deleted and the user is removed from the GroupWise system.

1 (Conditional) If the user owns library documents, see "Ensuring that a User's Library Documents Remain Accessible" on page 475 before deleting the user.
2 (Conditional) If the user owns resources, transfer the resources to another user in the same post office.
3 Ensure that the user has exited the GroupWise client and GroupWise Notify.
4 Ensure that the POA for the user's post office is running.

   If the POA is not running, the user mailbox is not deleted until the next time the POA runs.
5 In the GroupWise Admin console, browse to and click the name of the user you want to delete.
6 Click **More > Delete**.
7 Click **Yes** to confirm the deletion.
8 (Conditional) If the user was originally imported from an LDAP directory, delete the user from the LDAP directory.

To delete multiple accounts:

1 Click **Users**, select multiple users, then click **Delete**.

Ensuring that a User's Library Documents Remain Accessible

When you delete a user's GroupWise account, GroupWise does not delete any library documents to which the user has Author or Creator status. These documents remain in the library as "orphaned" documents, meaning that no one can access the documents.

If you or other users need access to the documents, you have the following choices:

- Change the mailbox password so that the user cannot log in. Other users can continue accessing the documents, and you can log in with the new password to manage the documents. For instructions, see "Creating or Changing a Mailbox Password" on page 470.
- Disable the user's ability to log in. For instructions, see "Disabling and Enabling GroupWise Accounts" on page 473.
- Change the mailbox to an inactive account. For instructions, see "Forcing Inactive Status" on page 474.
- Delete the user, then reassign the orphaned documents to another user. For instructions, see "Analyzing and Fixing Library and Document Information" on page 408.

Expiring a GroupWise Account

Rather than delete a user's GroupWise account, you can expire the account. The account, including the user's mailbox and all items, remains in GroupWise but cannot be accessed by the user. If necessary, the user's account can be reactivated at a later date. For more information, see "Managing Expired or Expiring GroupWise Accounts" on page 475.

This option is useful for providing GroupWise accounts to temporary or contract employees who come and go. You can set a user's GroupWise account to expire immediately or at a future date and time.

1 Ensure that the user has exited the GroupWise client and GroupWise Notify.

2 In the GroupWise Admin console, browse to and click the name of the user.

3 On the **Account** tab, select **Expiration Date**, then set the date to expire the account.

4 Click **Save**, then click **Close** to return to the main Admin console window.

Managing Expired or Expiring GroupWise Accounts

Expired GroupWise accounts remain expired until you reactivate them or delete them. Refer to the following sections for information to help you manage expired accounts:

- "Identifying Expired or Expiring Accounts" on page 476
- "Changing an Account's Expiration Date" on page 476
- "Reactivating an Expired Account" on page 476

Identifying Expired or Expiring Accounts

Rather than search for expired or expiring accounts, you can use the Expired Records tool to quickly list expired accounts for your entire system, a single domain, or a single post office. Depending on the date you choose, you can see expired accounts only or both expired and expiring accounts.

1 In the GroupWise Admin console, click **System > Expired Accounts**.

   or

   Browse to and click the name of a post office or domain, click the **Objects** tab, then click **Expired Accounts**.

   The **Expired As Of** field defaults to the current date. Only accounts that have expired as of this date are displayed in the list. To see accounts that will expire in the future, you need to change the date in the **Expired As Of** field.

   For example, in the dialog box shown above, the current date is 4/1/18 (April 1, 18). To see what accounts will expire by May 1, 18, you would change the **Expired As Of** date to 5/1/18.

2 When you are finished viewing expired or expiring accounts, click **Close**.

Changing an Account's Expiration Date

1 In the GroupWise Admin console, browse to and click the name of the user.

2 On the **Account** tab, click the **Calendar** icon located next to the **Expiration Date** field, then change the time and date.

3 Click **Save**, then click **Close** to return to the main Admin console window.

Reactivating an Expired Account

1 In the GroupWise Admin console, browse to and click the name of the user.

2 On the **Account** tab, deselect **Expiration Date**.

3 Click **Save**, then click **Close** to return to the main Admin console window.

54 Configuring Single Sign-On

GroupWise 18 supports single sign-on with KeyShield, eDirectory, Active Directory, and CASA.

Configuring Single Sign-On with KeyShield

GroupWise 18 supports KeyShield's single sign-on capabilities, allowing users to bypass logins by virtue of logging in once with KeyShield. This is enabled through the KeyShield client on a workstation. For more information on KeyShield, please visit their website (http://www.keyshieldsso.com/).

System Requirements

- The LDAP servers for GroupWise and KeyShield must be the same.
- Your GroupWise Post Offices, KeyShield server, and workstations must be time synced.
- You must be running KeyShield 6.0.2 or higher.
- You must be running GroupWise 18 or higher.

Configuring KeyShield SSO

1. (Conditional) If KeyShield is protected by APIKeys, create an API authorization for GroupWise in the KeyShield SSO console > **Configuration** > **API** > **API Authorizations**.
2. On the **Configuration** > **API** > **API Configuration** page, if you want to use HTTPS, upload PKCS#12 keystore file from the KeyShield server to generate a certificate.

   or

   On the **Configuration** > **API** > **API Configuration** page, generate a self signed certificate.
3. (Optional) Modify the **API Certificate validity** and **API Certificate notBefore** parameters as needed.
4. Apply the certificate configuration so the certificate is generated. Return to the **API Configuration** page edit mode and click **Download** next to the keystore name field.
5. In the GroupWise Admin console, go to System > System Preferences and upload the certificate in the **KeyShield SSO Certificate** field.

   The certificate is replicated to all GroupWise POAs.
6. In the GroupWise Admin console, enable **KeyShield SSO** on the **Client Options** > **Security** page of the Domain, Post Office, or User where you are using KeyShield.
7. (Optional) To use KeyShield with Web Access, the `KeyShield SSO Options` must be enabled in the `webacc.cfg` file on the Web Access server.

Configuring Single Sign-On with Active Directory

GroupWise 18 supports Active Directory's single sign-on capabilities allowing users to bypass the GroupWise login process by virtue of logging in once with Active Directory. Make sure the following tasks are completed before continuing with the configuration of the server:

- ❒ Make sure both the POA Server and the user workstation are joined to the same Active Directory domain.
- ❒ Make sure the POA has the DNS name specified instead of the IP address in the **GroupWise Admin Console** > **Post Office Agents** > *select the POA* > **Agent Settings** > **TCP/IP Address** field.
- ❒ Enable **LDAP Authentication** in the **GroupWise Admin Console** > **Post Offices** > *select the PO* > **Security** tab.
- ❒ Select **Network authentication (eDirectory or Active Directory)** in the **Admin Console** > **Post Office Agents** > *select the POA* > **Client Options** > **Security** tab.

Windows POA

If you are using NT LAN Manager (NTLM) single sign-on, then no further configuration is required on the POA server. Complete the tasks below if you are using Kerberos single sign-on:

- ❒ Register the POA as a Service Principle Name (SPN) by running the following command:

  ```
  gwadminutil adsso -a <path to post office directory>
  ```

  Example: `gwadminutil adsso -a M:\mypo`
- ❒ Create a Service Connection Point (SCP) record to allow the client to automatically connect to the POA. If you do not run this command, users need to know the IP address and port number to connect to the POA. Run the following command to create the SCP:

  ```
  gwadminutil adsso -scp -a <path to post office directory>
  ```

Linux POA

Complete the tasks below to enable Kerberos single sign-on.

- ❒ Make sure that all krb5 rpms are installed on the server.
- ❒ Make sure that the Linux server points to the AD server as its DNS server.
- ❒ Join the Linux POA server to the windows domain by configuring the YaST2 > Network Services > Windows Domain Membership applet. The **Kerberos Method** in the **Advanced Settings** or **Expert Settings** needs to be **system keytab**.
- ❒ Configure Kerberos by editing the `/etc/krb5.conf` file using the documentation for your version of SLES:
  - SLES 11
  - SLES 12
- ❒ Add GroupWise to the keytab file for Kerberos by running the following command:

  ```
  net ads keytab add groupwise
  ```

- ❐ Make sure that the `/etc/krb5.keytab` file is readable by the user that is running the GroupWise POA on the server. If it is not, do one of the following:
  - Change the ownership of the file to the same user as the user running the POA.
  - Add the POA user to a group and give the group read rights to the file.
- ❐ Create a GroupWise Name Server in DNS to allow the client to automatically connect to the POA. If you do not do this, users need to know the IP address and port number to connect to the POA.

Enabling eDirectory and CASA Single Sign-on

By default, if a user must enter a password when logging in to GroupWise, he or she is prompted for the password.

The GroupWise client includes several options that users can choose from to enable them to log in without providing a password. These options, located on the Security Options dialog box (GroupWise client > **Tools** > **Options** > **Security**), are described in the following table:

GroupWise Client Option	Description
No Password Required with eDirectory	This option is available only when logged in to NetIQ eDirectory. When GroupWise starts, it automatically logs in to the GroupWise account associated with the user who is logged in to eDirectory at the workstation. No GroupWise password is required.
Use Single Sign-On	This option is available only when using Micro Focus Single Sign-on 2.0 and SecureLogin 3.0 and later products. When GroupWise starts, it uses the GroupWise password stored by Micro Focus Single Sign-on or SecureLogin.
Use Collaboration Single Sign-On (CASA)	This option is available only when using Micro Focus Common Authentication Services Adapter (CASA) 1.0 and later. When GroupWise starts, it uses the GroupWise password stored by Micro Focus CASA.

As shown in the table, these options appear only if certain conditions are met, such as the user having Micro Focus Single Sign-on or SecureLogin installed. If you don't want the option to be available to users even if the condition is met, you can disable the option. Doing so removes it from the GroupWise client's Password dialog box.

To disable one or more of the password options:

1. In the GroupWise Admin console, browse to and click the name of a domain, post office, or user.
2. With the appropriate GroupWise object selected, click **Client Options** to display the GroupWise Client Options dialog box.
3. Click the **Security** tab.
4. Select **Use eDirectory Authentication Instead of Password** if you want NetIQ eDirectory users to be able to use the GroupWise client's **No Password Required with eDirectory** option.

   This option is available only if LDAP authentication is enabled for the post office. For more information, see "Configuring Post Office Security" on page 150.
5. Deselect **Enable Single Sign-on** if you don't want Single Sign-on or SecureLogin users to be able to use the GroupWise client's **Use Micro Focus Single Sign-on** option.

6 Select **Use Collaboration Single Sign-On (CASA)** if you want users of Micro Focus collaboration products (GroupWise, Messenger, iFolder, and iPrint) to be able to use the same password for all collaboration products.

7 Click **OK** to save your changes.

X Groups

55 Understanding Groups

Groups are sets of users (and optionally, resources and other groups) that can be addressed as a single entity. When a GroupWise user addresses an item (message, appointment, task, or note) to a group, each user or resource that is a member receives the item if he or she has a GroupWise account.

The following sections provide information to help you learn about groups:

Personal Groups

GroupWise users can create personal groups in the GroupWise client. When a user creates a personal group, the group is saved in the user's mailbox and is available for use only by that user. A personal group cannot be shared by, or transferred to, other users. For more information about personal groups, see "Managing Groups" in the *GroupWise 18 Client User Guide*.

GroupWise Groups

A GroupWise group is group that you, as the GroupWise administrator, create to facilitate easier addressing within your GroupWise system. Each group that you want to create must be added as a Group object in the GroupWise Admin console. The name that you give the Group object becomes the name by which the group is displayed in the GroupWise Address Book.

A group can consist of users, resources, and other groups. Members do not need to be in the same post office as the group's post office.

Because a group is an addressable entity, you must assign it to a post office when you create it. Regardless of the group's post office, all GroupWise users can use the group when addressing a message.

LDAP Groups

LDAP groups are objects in an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory that can be created to facilitate easier administration of LDAP users who have common needs or who share a common role or responsibility.

LDAP groups are administered in the associated LDAP directory. eDirectory groups are administered in iManager. Active Directory groups are administered in the Microsoft Management Console (MMC). GroupWise includes plugins for eDirectory and for MMC to enable LDAP administrators to add new LDAP groups to GroupWise in the administrative environment with which they are familiar. For information about installing and using the GroupWise plugins, see "Using an LDAP Directory Management Tool for Adding LDAP Users and Groups to GroupWise" on page 40.

The name that you give to the LDAP Group object in the LDAP directory management tool becomes the name by which it is displayed in the GroupWise Address Book. You make an LDAP group available in your GroupWise system by assigning it to a post office. Regardless of the post office where the LDAP group is assigned, all GroupWise users can use it when addressing a message.

After you add an LDAP group to GroupWise, you cannot change group membership in the GroupWise Admin console. Instead, you must use the same LDAP directory management tool to modify group membership as you used to create the LDAP group. Changes made in the LDAP management tool synchronize to GroupWise during the next scheduled LDAP sync.

Apart from modifying group membership, a group that was originally an LDAP group and a native GroupWise group can be managed essentially the same.

56 Creating and Managing Groups

A GroupWise group can contain GroupWise users, resources, and other groups. When creating the group, you can determine each member's participation in the group (primary recipient, courtesy copy recipient, or blind copy recipient). Groups are displayed in the GroupWise Address Book. When a GroupWise user addresses an item (message, appointment, task, or note) to a group, each user or resource that is a member receives the item if he or she has a GroupWise account.

Creating a New Group

1 In the GroupWise Admin console, click **Groups > New**.

2 Specify a unique name for the group. Do not use any of the characters listed in "Invalid Characters in GroupWise Object Names and Email Addresses".

> **IMPORTANT:** Characters that are valid and even desirable in a group name, such as accented characters, might not be valid in an email address. For some groups you might need to set up a preferred email ID in order to ensure that they have a valid email address. For instructions, see "Changing a Group's Internet Addressing Settings" on page 489.

3 Select the post office the group will be assigned to.

The group can contain members of other post offices.

4 Click **OK** to create the group and add it to the list of groups.

5 Continue with Adding Members to a Group.

Adding Members to a Group

Groups can contain users, resources, and other groups.

> **NOTE:** If the group is being synchronized from an LDAP group, you cannot modify group membership in the GroupWise Admin console. Instead, you must use the same LDAP directory management tool to modify group membership that you used to create the LDAP group. Changes to membership in the LDAP group automatically synchronize to the GroupWise group.

1 In the GroupWise Admin console, browse to and click the name of the group.

2 Click **Add** to add members to the group:

2a Select **Users** to list and select users, then click **OK**.

2b Select **Resources** to list and select resources, then click **OK**.

2c Select **Groups** to list and select groups, then click **OK**.

You cannot select more than one type of object at a time.

By default, all users are given **To** participation.

3 To change the participation of members to CC or BC, select the members, click **Participation**, then select **CC** or **BC**.

4 Click **Save**, then click **Close** to return to the main Admin console window.

5 Continue with Configuring a New Group.

Groups are typically managed by an administrator in the GroupWise Admin console. In addition, users can be granted rights to modify groups. For instructions, see "Enabling Users to Modify a Group" on page 488.

As an alternative, GroupWise client users can create shared address books and then create groups within those shared address books, so that the groups are available to all users with whom the address book has been shared. The creator of the shared address book can give other users read-only rights, or can choose to grant them additional rights for adding, editing, and deleting information. For more information about shared address books, see "Sharing an Address Book with Another User" in the *GroupWise 18 Client User Guide*.

Configuring a New Group

1 In the GroupWise Admin console, browse to and click the name of a new group.

2 Click the **General** tab.

3 (Optional) Modify any of the following fields on the **General** tab:

Description: Specify a description to help you identify the purpose or members of the group.

Visibility: Select the level at which the group will be visible in the GroupWise Address Book. For more information, see "Controlling Object Visibility" on page 72.

Replication Override: By default, groups are replicated throughout your GroupWise system based on the selected visibility level. With the default visibility level, groups are visible in the GroupWise Address Book for local post office users only and are not replicated to other post offices.

If you set Visibility to **Domain**, the group is replicated to all post offices in the domain, but not to post offices belonging to other domains. If you set Visibility to **System**, the group is replicated to all post offices in your GroupWise system. This default behavior corresponds to the **Replicate According to Visibility** setting.

Select **Replicate Everywhere Regardless of Visibility** if you want the group replicated throughout your GroupWise system regardless of the selected visibility level. With this setting, the group is made available in all post offices, although it is still only visible in the GroupWise Address Book according to the selected visibility level. The availability of the group in all post offices means that it can be nested into other groups that are visible in any post office, and that users in any post office can manually specify the group name in the **To** field of an item.

Email Address: Displays the email address for the group.

4 (Optional) Click the **Nicknames** tab to define one or more nicknames for the group.

For more information, see Part XII, "Nicknames," on page 501.

5 (Optional) Click the **Internet Addressing** tab to customize the group's email address information.

For more information, see "Overriding Internet Addressing" on page 278.

6 (Optional) Click the **Access Control** tab to grant to users the right to modify the group in the GroupWise client or to send to a restricted group.

For more information, see "Controlling Access to a Group" on page 488 and "Enabling Users to Modify a Group" on page 488.

7 Click **Save**, then click **Close** to return to the main Admin console window.

Removing Members from a Group

When you remove users' or resources' GroupWise accounts or delete groups, they are automatically removed from any groups in which they have membership.

NOTE: If the group is being synchronized from an LDAP group, you cannot modify group membership in the GroupWise Admin console. Instead, you must use the same LDAP directory management tool to modify group membership that you used to create the LDAP group. Changes to membership in the LDAP group automatically synchronize to the GroupWise group.

To manually remove members from a group:

1. In the GroupWise Admin console, browse to and click the name of a group.
2. On the **Membership** tab, select one or more members that you want to remove from the list, then click **Delete**.

Moving a Group

If necessary, you can move a group from one post office to another. For example, you might need to move a group from a post office you are removing.

The group retains the same name in the new post office as it has on the current post office. If another user, resource, or group assigned to the new post office has the same name, you must rename one of them before you move the group. For details, see "Renaming a Group" on page 487.

1. In the GroupWise Admin console, browse to and click the name of the group.
2. Click **More > Move**.
3. Select the post office to which you want to move the group.
4. (Optional) Create a nickname for the group so that messages that will be undeliverable at the original post office location are successfully delivered to the new post office location.

   For more information, see Part XII, "Nicknames," on page 501.
5. Click **OK** to move the group.

Renaming a Group

Situations might arise where you need to give a group a new name. For example, you might need to move the group to another post office that already has a user, resource, or group with the same name.

To rename a group:

1. In the GroupWise Admin console, browse to and click the name of the group.
2. Click **More > Rename**.
3. Specify the new name for the group.
4. Click **OK** to rename the group.

Controlling Access to a Group

By default, all GroupWise users can send to all GroupWise system-level groups that appear in the GroupWise Address Book. If necessary, you can restrict which users are allowed to send to a specific group. The restricted group still appears in the GroupWise Address Book, but if unauthorized users try to send to the restricted group, they receive an error indicating that they do not have the rights to use the restricted group.

To restrict access to a group:

1. In the GroupWise Admin console, browse to and click the name of the group.
2. Click the **Access Control** tab.
3. Click **Add**, select one or more users who are allowed to send to the restricted group, then click **OK** to add the users to the Access Control list.
4. (Optional) Click **Add**, select **Resources**, select one or more resources that are allowed to send to the restricted group, then click **OK** to add the resources to the Access Control list.
5. (Optional) Click **Add**, select **Groups**, select one or more groups that are allowed to send to the restricted group, then click **OK** to add the groups to the Access Control list.

   IMPORTANT: After you add users, resources, and groups to the Access Control list, only those users, resources, and groups can send to the restricted group.

6. Click **Save**, then click **Close** to return to the main Admin console window.
7. Notify the users that they have rights to send to the restricted group.

In addition to the users that you add to the Access Control list, users to whom you have granted edit rights can also send to the restricted group, even if you do not explicitly add them to the Access Control list. For more information, see "Enabling Users to Modify a Group" on page 488.

Enabling Users to Modify a Group

In the GroupWise Admin console, you can grant rights to users to modify GroupWise system-level groups in the GroupWise client. However, users cannot create or delete GroupWise system-level groups in the client. That task can be done only in the GroupWise Admin console by an administrator.

Selecting the Users Who Can Modify a Group

To select users who can modify a GroupWise system-level group:

1. In the GroupWise Admin console, browse to and click the name of the group.
2. Click the **Access Control** tab, then locate the **People Who Can Modify This Group** section.
3. Click **Add**, then select one or more users who can edit the group.
4. Click **OK** to grant the edit rights.
5. Notify the users that they have rights to modify the group.

Granting Group Modification Rights to a User

To give a specific user rights to edit one or more GroupWise system-level groups:

1. In the GroupWise Admin console, browse to and click the name of user.

2 Click the **Objects** tab, then click **Group Administration**.

3 Click **Add**, then select one or more system-level groups for the user to edit.

4 Click **Save**, then click **Close** to return to the main Admin console window.

5 Notify the user that he or she has rights to modify the system-level groups.

In the GroupWise client, the editable group does not appear any different to the user who has rights to edit it, except that **Add** and **Remove** are active for that user.

In Online mode, the user can edit the group in the GroupWise Address Book. In Caching mode, the user cannot edit the group in the GroupWise Address Book. However, the user can edit the group in the Address Selector in a new message.

Deleting a Group

To delete a single group:

1 In the GroupWise Admin console, browse to and click the name of the group.

2 Click **Delete**.

3 Click **Yes** to confirm the deletion.

To delete multiple groups that belong to the same post office:

1 In the GroupWise Admin console, browse to and click the name of the post office.

2 Click the **Objects** tab, then click **Groups**.

3 Select one or more groups, then click **Delete**.

4 Click **OK** to complete the deletion.

NOTE: If the group was being synchronized from an LDAP group, deleting the GroupWise group in the GroupWise Admin console does not delete the LDAP group in the LDAP directory. If the group no longer serves a purpose in the LDAP directory, you must use the same LDAP directory management tool to delete the group that you used to create the group.

Managing Email Addresses

To ensure that group addresses meet your needs, GroupWise enables you to determine the format and visibility of addresses, as well as create additional names for groups. The following sections provide details:

Changing a Group's Internet Addressing Settings

By default, a group inherits its Internet address settings (preferred Internet address format, allowed address formats, and Internet domain name) from its post office, domain, or GroupWise system. If necessary, you can override these settings for a group. For more information, see "Overriding Internet Addressing" on page 278.

Changing a Group’s Visibility in the Address Book

A group’s visibility level determines which users see the group in the Address Books. You can control the availability of a group by displaying it in the Address Book for all users in your GroupWise system, in the Address Book for those users in the group’s domain only, in the Address Book for those users on the group’s post office only, or not displaying it at all. For more information, see “Controlling Object Visibility” on page 72

Adding External Users to a Group

Members of groups must have GroupWise accounts. If you want to add users to a group, and the users do not belong to your GroupWise system, you must create objects to represent these external users within your GroupWise system. For more information, see Chapter 11, “Using an External Domain to Represent Another Email System,” on page 109.

XI Resources

57 Creating Resources

A resource is an item or place, such as a computer, company vehicle, or conference room, that users can schedule or check out. A resource can also be a role that different users might have at different times.

Understanding Resources

Resource Objects

Each resource that you want to make available must be added as a Resource object in your GroupWise system. The name that you give the Resource object becomes the name by which the resource is displayed in the GroupWise Address Book.

Although you can import users and groups from an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory, you cannot import LDAP resources.

Resource Types

You can identify the resource as a general resource, as a place, or as a role.

When a user schedules a resource that is defined as a place, the resource name is automatically added to the **Place** field in the appointment.

Starting in GroupWise 2012 SP2, a role resource represents a position in an organization that can be reassigned from one owner to the next. As owners change, the role resource mailbox retains all information associated with the role. Unlike general resources and place resources, role resources are included in a Reply to All.

Resource Mailboxes

Like a user, a resource must be assigned to a post office so that it can be given an account (address, mailbox, and so on). You assign the resource to a post office when you create the Resource object.

A resource's account enables it to receive scheduling requests (sent as appointments). The owner assigned to the resource can access the resource's mailbox to accept or decline the requests. For example, you might want to have all your conference rooms defined as place resources. When sending a meeting appointment, users can schedule the conference room as well as the meeting attendees. The place resource, just like the other users scheduled for the meeting, receives an appointment in its mailbox which can be accepted or declined by the owner.

When scheduling a resource, users can perform a busy search to see when the resource is available. Even though a resource is assigned to a single post office, all users in your GroupWise system can schedule the resource.

Resources can receive all item types (mail messages, phone messages, appointments, tasks, and notes). Generally, if your purpose in defining resources is to allow them to be scheduled through GroupWise, they only receive appointments.

Resources can also send items. If a resource sends an item to an Internet user, both the **To** field and the **From** field are populated with the resource name when the Internet user receives the message.

Resource Owners

When you create a resource, you assign an owner to it. The owner must belong to the same post office as the resource and is responsible for accepting or declining requests to schedule the resource. The owner can do this by proxying to the resource's mailbox and opening the scheduling requests, or by setting up rules to manage the resource automatically. For more information, see "Creating Rules for a Resource" on page 497.

The owner automatically receives proxy rights to the resource's mailbox. The owner can also grant proxy rights to another user to manage the resource.

The owner cannot log in directly to the resource mailbox. However, the owner can set a password on the resource mailbox to facilitate secure access by an IMAP client. After proxying in to the resource mailbox, click **Tools > Options > Security > Password** to set a password on the resource mailbox.

For more information about how owners can manage resources, see "Managing Resources" in the *GroupWise 18 Client User Guide*.

Planning Resources

Before creating a new resource, ensure that the user who will own the resource has been created and belongs to the same post office where you are planning to create the resource.

Creating a New Resource

1 In the GroupWise Admin console, click **Resources,** then click **New** to display the Create GroupWise Resource dialog box.

2 Fill in the following fields:

   Resource Name: Specify a descriptive name. Because the name is used as part of the resource's GroupWise email address, do not use any invalid characters in the resource name. For more information, see "Invalid Characters in GroupWise Object Names and Email Addresses".

   IMPORTANT: Characters that are valid and even desirable in a resource name, such as accented characters, might not be valid in an email address. For some resources, you might need to set up a preferred email ID in order to ensure that they have a valid email address. For instructions, see "Changing a Resource's Internet Addressing Settings" on page 500.

   GroupWise Post Office: Select the post office where the resource will be located.

   Owner: Select the user who will be responsible for accepting or declining requests to use the resource. The owner must have a GroupWise account on the same post office as the resource.

3 Click OK to create the resource.

4 Click **Save**, then click **Close** to return to the main Admin console window.

5 Continue with Configuring the New Resource.

Configuring the New Resource

1. In the GroupWise Admin console, browse to and click the name of the new resource.
2. (Optional) Modify any of the following fields on the **General** tab:

   File ID: This three-letter ID is randomly generated and is non-editable. It is used for various internal purposes within the GroupWise system, including ensuring that files associated with the resource have unique names.

   Owner: Select the user who will be responsible for accepting or declining requests to use the resource. The owner must have a GroupWise account on the same post office as the resource.

   Description: Specify a description to help users identify the use of the resource. The description is displayed if the user chooses to view information about the resource in the GroupWise Address Book.

   If you define the resource type as a place, the description is automatically added to the **Place** field in the appointment. A good description can help users locate the place more easily.

   Visibility: Select the level at which the resource will be visible in the GroupWise Address Book. For more information, see "Controlling Object Visibility" on page 72.

   Resource Type: You can identify the resource as a general resource, as a place, or as a role. When a user schedules a place resource, the resource description is automatically added to the **Place** field in the appointment. A role resource is treated more like a user than a general resource or a place resource, and can be included in a Reply to All.

   Phone: If the resource has a telephone number associated with it, such as a conference room with a telephone number, specify the phone number.

   Email Address: Displays the email address for the resource.

   Restore Area: This field applies only if you are using the GroupWise backup and restore features. If so, this field indicates the location where the resource's mailbox is being backed up. For details, see Chapter 49, "Restoring GroupWise Databases from Backup," on page 423.

   Expiration Date: If you want the resource's GroupWise account to no longer work after a certain date, specify the expiration date. For more information, see "Expiring a GroupWise Account" on page 475.
3. (Optional) Click the **Nicknames** tab to define one or more nicknames for the resource.

   For more information, see Part XII, "Nicknames," on page 501.
4. (Optional) Click the **Internet Addressing** tab to customize the resource's email address information.

   For more information, see "Overriding Internet Addressing" on page 278.
5. (Optional) If you do not want to manually manage the resource, see "Creating Rules for a Resource" on page 497.
6. Click **Save**, then click **Close** to return to the main Admin console window.

58 Managing Resources

A resource's mailbox, just like a user's mailbox, is a combination of the information stored in its user database and the message databases located at its post office. Occasionally, you might want to perform maintenance tasks on the resource's mailbox to ensure the integrity of the databases. For details about performing maintenance on a resource's mailbox, see Chapter 43, "Maintaining User/Resource and Message Databases," on page 403.

Creating Rules for a Resource

Schedulable resources such as conference rooms need effective auto-accept/decline rules to help compensate for times when appointment schedulers fail to use Busy Search.

If you are the resource owner, you can proxy to the resource mailbox in order to set up the rules. If you are not the resource owner, be sure that the resource owner understands how to set up effective rules for the resource.

Creating an Auto-Accept Rule

Creating an auto-accept rule provides confirmation to the appointment scheduler that the resource as accepted the appointment.

1. In the GroupWise client, in the resource mailbox, click **Tools > Rules**, then click **New**.
2. Type a name for the auto-accept rule.
3. Select **Received**.
4. Select **Appointment**.
5. In the **Appointment conflict exists** drop-down list, select **No**.
6. Create an action to accept the appointment:
   - **6a** Click **Add Action**.
   - **6b** Click **Accept**.
   - **6c** Select a **Show As** setting.
   - **6d** (Optional) Type a comment to include with the acceptance.
   - **6e** Click **OK**.
7. Create an action to notify the appointment scheduler that the resource has accepted the appointment:
   - **7a** Click **Add Action**.
   - **7b** Click **Reply**.
   - **7c** Click **OK** to accept the default of replying only to the appointment scheduler.
   - **7d** In the **Subject** field, indicate that the resource has accepted the appointment.
   - **7e** (Optional) In the **Message** field, provide any additional information that might be helpful to the appointment scheduler.
   - **7f** Click **OK**.

8 Test the rule by scheduling an appointment that includes the resource for a time when the resource is available.

9 Continue with Creating an Auto-Decline Rule.

Creating an Auto-Decline Rule

Creating an auto-decline rule notifies the appointment scheduler that the resource is not available. By notifying users in addition to the appointment scheduler, the likelihood of a perceived double-booking of the resource is minimized.

1 In the GroupWise client, in the resource mailbox, click **Tools > Rules**, then click **New**.

2 Type a name for the auto-decline rule.

3 Select **Received**.

4 Select **Appointment**.

5 In the **Appointment conflict exists** drop-down list, select **Yes**.

6 Create an action to decline the appointment:

   6a Click **Add Action**.

   6b Click **Delete/Decline**.

   6c (Optional) Type a comment about the resource declining the appointment.

   6d Click **OK**.

7 Create an action to notify the appointment scheduler that the resource has declined the appointment:

   7a Click **Add Action**.

   7b Click **Reply**.

   7c Click **OK** to accept the default of replying only to the appointment scheduler.

   or

   Select **Reply to all (sender and recipients)** to ensure that everyone involved with the appointment is notified that the resource has declined the appointment.

   7d In the **Subject** field, indicate that the resource has declined the appointment.

   7e (Optional) In the **Message** field, provide any additional information that might be helpful to the appointment scheduler.

   7f (Optional) In the **CC** field or the **BC** field, include one or more additional users such as the resource owner to notify when a resource declines an appointment.

   7g Click **OK**.

8 Test the rule by scheduling an appointment that includes the resource for a time when the resource is not available.

Changing a Resource’s Owner

You can change a resource’s owner whenever necessary. The owner must be a user assigned to the same post office as the resource. If you need to give ownership of the resource to a user on a different post office, you must move the resource to that post office. For details, see “Moving a Resource” on page 499.

The new owner automatically receives proxy rights to the resource’s mailbox. Proxy rights are removed for the old owner.

Ensure that the new resource owner understands the auto-accept/decline rules that are associated with the resource.

1. In the GroupWise Admin console, browse to and click the name of the resource.
2. Click the **General** tab, then locate the **Owner** field.
3. Select the new owner from the drop-down menu, then click **OK** to display the user's name in the **Owner** field.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Adding a Resource to a GroupWise Group

Just like users, resources can be added to groups.

1. In the GroupWise Admin console, browse to and click the name of the resource.
2. Click the **Groups** tab.
3. Click **Add**, select one or more groups that you want to add the resource to, then click **OK**.

   By default, the resource is added as a primary recipient (**To** recipient).
4. (Conditional) If you want to change the resource's recipient type, select the group, click **Participation**, then click **To**, **CC**, or **BC**.
5. Click **Save**, then click **Close** to return to the main Admin console window.

Moving a Resource

If necessary, you can move a resource from one post office to another. For example, you might need to move a resource if you are removing the resource's post office, or if you need to reassign ownership of the resource to a user on another post office.

The resource retains the same name in the new post office as it has in the current post office. If another user, resource, or group assigned to the new post office has the same name, you must rename one of them before you move the resource. For details, see "Renaming a Resource" on page 500.

When you move the resource, all items in its mailbox are moved to the new post office, which means that all schedules for the resource are kept intact.

1. In the GroupWise Admin console, browse to and click the name of the resource.
2. Click **More > Move**.
3. Select the post office to which you want to move the resource.
4. (Optional) Select **Create Nickname(s) for the Selected Object(s)**, so that messages that will be undeliverable to the old email address are successfully delivered to the new email address.

   For more information, see Part XII, "Nicknames," on page 501.
5. Click **OK** to display the Choose New Owner dialog box.
6. Select the user who will be the resource's owner, then click **OK** to move the resource.

Renaming a Resource

Situations might arise where you need to give a resource a new name. For example, you might need to move the resource to another post office that already has a user, resource, or group with the same name.

1 In the GroupWise Admin console, browse to and click the name of the resource.
2 Click **More > Rename**.
3 In the **New GroupWise Name** field, specify the new name for the resource.
4 (Optional) Select **Create Nickname for This Object**, so that messages that will be undeliverable to the old email address are successfully delivered to the new email address.

   For more information, see Part XII, "Nicknames," on page 501.
5 Click **OK** to rename the resource.

Deleting a Resource

When you delete a resource, all information is removed for the resource, including any schedules that have been established for the resource.

1 In the GroupWise Admin console, browse to and click the name of the resource.
2 Click **More > Delete**.
3 Click **Yes** to confirm the deletion.

Managing Resource Email Addresses

To ensure that resource addresses meet your needs, GroupWise enables you to determine the format and visibility of addresses, as well as create additional names for resources. The following sections provide details:

Changing a Resource's Internet Addressing Settings

By default, a resource inherits its Internet address settings (preferred Internet address format, allowed address formats, and Internet domain name) from its post office, domain, or GroupWise system. If necessary, you can override these setting for a resource. For more information, see "Overriding Internet Addressing" on page 278.

Changing a Resource's Visibility in the Address Book

A resource's visibility level determines which users see the resource in their Address Books. You can control the availability of a resource by displaying it in the Address Books of all users in your GroupWise system, in the Address Books of those users in the resource's domain only, in the Address Books of those users on the resource's post office only, or in no Address Books. Even if the resource is not displayed in their Address Books, users can schedule the resource if they know the resource's name. For more information, see "Controlling Object Visibility" on page 72.

XII Nicknames

59 Understanding Nicknames

A nickname is an additional object name for a user, resource, or group that facilitates message delivery and controls the object's availability in the GroupWise Address Book. Nicknames can be manually established on the Nickname tab of User, Group, and Resource objects. They can also be generated when you rename an object or move an object to a different post office. The nickname gives the object an additional email address.

Nicknames are useful in the following situations:

- You rename a user, resource, or group. You can create a nickname that retains the original object name, so that messages with the original object name in the email address are routed to the new email address. You can configure the GroupWise Admin console to prompt for or automatically create nicknames when you rename objects.
- You move a user, resource, or group. You can create a nickname that retains the old post office location. As messages to the moved object arrive in your GroupWise system, the email address is routed to the new post office location. You can configure the GroupWise Admin console to prompt for or automatically create nicknames when you move objects.
- You need to restrict the visibility of a user, resource, or group in the GroupWise Address Book, but you need to make the object visible in one or more specific Address Books outside of the restricted visibility. You can create a nickname that provides the specific visibility that is ruled out by the required restriction. For more information about visibility, see "Controlling Object Visibility" on page 72.

You can retain a nickname permanently, or you can configure it to expire after a specified amount of time.

In the GroupWise Admin console, you can list all the nicknames in your GroupWise system by clicking **Nicknames** in the Administration panel. In the GroupWise client, you can display nicknames in the GroupWise Address Book if you enable **Filter for Contacts**. When addressing a message, users need to know a nickname in order to use it.

60 Manually Creating Nicknames

Manually Creating a Nickname for a User

To create a nickname for a user:

1. In the GroupWise Admin console, browse to and click the user name, click the **Objects** tab, click **Nicknames**, then click **New**.
2. Fill in the following fields:

   Nickname: Specify a unique user name. Do not use any of the characters listed in "Invalid Characters in GroupWise Object Names and Email Addresses".

   First Name: (Optional) Specify the user's first name or given name.

   Last Name: (Optional) Specify the user's last name or surname.

   Post Office: Select the post office that you want to own the nickname. This can be any post office in your GroupWise system; it does not need to be the user's post office.

   Visibility: Select the Address Book visibility for the nickname. This determines where the nickname is available (system, domain, post office, or none). However, nicknames are not displayed in the Address Book unless you filter for them. In order to address a message to a nickname, a user must specify the nickname address, and the nickname must be available in the user's post office.

   Expiration Date: If you want the nickname to be removed by the Expire Records feature after a certain date, select **Expiration Date**, then select the desired date.

   For more information, see "Managing Expired or Expiring GroupWise Accounts" on page 475.
3. Click **OK** to add the nickname to the list.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Manually Creating a Nickname for a Resource

To create a nickname for a resource:

1. In the GroupWise Admin console, browse to and click the resource name, click the **Nicknames** tab, then click **New**.
2. Fill in the following fields:

   Nickname: Specify a unique name for the resource. Do not use any of the characters listed in "Invalid Characters in GroupWise Object Names and Email Addresses".

   First Name: (Not applicable for a resource.)

   Last Name: (Not applicable for a resource.)

   Post Office: Select the post office that you want to own the nickname. This can be any post office in your GroupWise system; it does not need to be the post office that owns the resource.

Visibility: Select the Address Book visibility for the nickname. This determines where the nickname is available (system, domain, post office, or none). However, nicknames are not displayed in the Address Book unless you filter for them. In order to address a message to a nickname, a user must specify the nickname address, and the nickname must be available in the user's post office.

Expiration Date: If you want the nickname to no longer work after a certain date, click **Expiration Date**, then select the desired date.

3. Click **OK** to add the nickname to the list.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Manually Creating a Nickname for a Group

To create a nickname for a group:

1. In the GroupWise Admin console, browse to and click the group name, click the **Nicknames** tab, then click **New**.
2. Fill in the following fields:

   Fill in the following fields:

   Nickname: Specify a unique name for the group. Do not use any of the characters listed in "Invalid Characters in GroupWise Object Names and Email Addresses".

   First Name: (Not applicable for a group.)

   Last Name: (Not applicable for a group.)

   Visibility: Select the Address Book visibility for the nickname. This determines where the nickname is available (system, domain, post office, or none). However, nicknames are not displayed in the Address Book unless you filter for them. In order to address a message to a nickname, a user must specify the nickname address, and the nickname must be available in the user's post office.

   Expiration Date: If you want the nickname to no longer work after a certain date, click **Expiration Date**, then select the desired date.
3. Click **OK** to add the nickname to the list.
4. Click **Save**, then click **Close** to return to the main Admin console window.

61 Configuring Automatic Nickname Creation

By default, the GroupWise Admin console offers you the opportunity to create a nickname whenever you move or rename a user.

You can configure the GroupWise Admin console so that nicknames are always created or never created whenever you move or rename objects.

1. In the GroupWise Admin console, click **System > System Preferences**, then click the **Settings** tab.
2. Select **Always** so that the **Create Nicknames** field is always selected and dimmed.

   or

   Select **Never** so that the **Create Nicknames** field is always deselected and dimmed.
3. Click **OK** to save the setting.

62 Managing Nicknames

Although you create nicknames on the objects that are affected by the nicknames, you can list all of the nicknames in your GroupWise system all at once.

1 In the GroupWise Admin console, click **Nicknames** in the **Administration** panel.

   When you move an object, the destination post office is listed. When you rename an object, both the original name (now the nickname) and the new name are listed.

2 To change the visibility of a nickname, click the nickname, then modify the **Visibility** field on the **General** tab as needed.

   For background information, see “Controlling Object Visibility” on page 72.

3 To check or change the expiration date of a nickname, click the nickname, then modify the **Expiration Date** field on the **General** tab as needed.

   For background information, see “Managing Expired or Expiring GroupWise Accounts” on page 475.

4 To set a preferred email ID for the nickname or make other email customizations for the nickname, click the nickname, click the **Internet Addressing** tab, then change settings as needed.

   For background information, see “Managing User Email Addresses” on page 471.

5 To delete a nickname, so that references to the original name are no longer recognized, select the nickname, then click **Delete**.

XIII Libraries and Documents

63 Document Management Services Overview

GroupWise Document Management Services (DMS) lets users create documents with integrated applications, save them, then easily locate a specific document later without knowing the application, a specific document name, or the document's physical location. Users can create, share, locate, edit, view, and check out documents that are created under the management of GroupWise DMS.

Libraries

A library is a set of documents and a database that allows the documents to be managed as a unit. A library must belong to a specific post office but can be accessed by users in other post offices. The GroupWise client enables users to store and manage their documents in the library. The GroupWise Post Office Agent (POA) transfers documents between the GroupWise client and the library.

In the GroupWise client, users can view a list of all the libraries to which they have access by clicking **Tools** > **Options** > **Documents**.

For complete information on libraries, see Chapter 64, "Creating and Managing Libraries," on page 515.

Document Storage Areas

Documents can be stored at the post office. This is the simplest configuration, but it is not recommended for libraries where substantial growth is anticipated because documents stored at the post office cannot easily be moved to a different location where additional storage space is available.

Preferably, documents should be stored outside the post office, in document storage areas. Document storage areas are physical locations, such as drive volumes, optical devices, hard drives on other servers, and so on. Document storage areas can be located anywhere that the POA can access them locally or using direct network access (mapped drive or mounted file system).

A document storage area has the same internal folder structure that is used to store documents at the post office. The only difference is that a document storage area can be located anywhere in your system. Therefore, a document storage area can be moved easily, so it is easy to expand your document storage capacity if you store documents in a document storage area rather than at the post office.

For complete information on document storage areas, see Section 65, "Managing Document Storage Areas in Libraries," on page 525.

Documents

Documents created using GroupWise DMS are not stored as individual files. Instead, documents are stored in database structures called binary large objects (BLOBs). A document and all of its versions are stored in the separate BLOB files. BLOBs are compressed (50% or more) to conserve storage space. BLOBs are encrypted to provide security.

For complete information on documents, see Chapter 66, “Creating and Managing Documents,” on page 527.

64 Creating and Managing Libraries

To use one or more libraries as part of your GroupWise system, perform the following tasks as needed:

IMPORTANT: If you are creating a new library in a clustered GroupWise system, see "Clustering" in the *GroupWise 18 Interoperability Guide* before you create the library.

Planning a Library

This section provides the information you need in order to set up a new library. "Library Worksheet" on page 523 lists all the information you need as you set up a library. You should print the worksheet and fill it out as you complete the sections below.

After you have completed the tasks and filled out the worksheet, you are ready to continue with "Creating a Library" on page 517.

Selecting the Post Office That the Library Will Belong To

If you are creating a new library for each post office in your GroupWise system, print a copy of "Library Worksheet" on page 523 for each post office.

If users in several post offices will store documents in the same library, you must decide which post office should own the library. A library can never be reassigned to a different post office, so you should choose the owning post office carefully. You should consider which users will use the library most frequently and where you might want to create additional libraries in the future.

LIBRARY WORKSHEET
Under **Post Office**, specify the name of the post office that will own the new library.

Choosing the Library Name

When you create the Library object, you must give the library a name. This is the name that is displayed in the GroupWise Admin console.

After you have specified the library's name and created the Library object, the name cannot be changed. Therefore, if you have or will have other libraries, you should pick a name that uniquely identifies the library. For example, use the name to identify the post office it is assigned to.

Do not use any invalid characters in the library's name. For more information, see "Invalid Characters in GroupWise Object Names."

By default, the library name that users see in the GroupWise client is the same as the Library object name. However, you can change the display name if you want it to be different from the Library object name.

LIBRARY WORKSHEET

Under **Library Name**, specify the Library object name.

Under **Library Description**, provide a brief description of the planned use for the library.

Under **Display Name**, specify the library name you want users to see in the GroupWise client, if it is different from the Library object name.

Deciding Where to Store Documents

You can store documents at the post office in the `post_office\gwdms\library\docs` subfolder of the post office. You can later add document storage areas outside the post office if DMS usage grows. However, the documents stored at the post office can never be moved.

A document storage area has the same internal folder structure that is used to store documents at the post office, but it can be located anywhere in your system. Document storage areas can be moved easily, so it is easy to expand your document storage capacity when you store documents in document storage areas rather than at the post office.

You might want to set up a document storage area on the same server where the POA runs so as not to increase network traffic. The POA can index and serve documents to users most efficiently if the document storage area is located locally.

LIBRARY WORKSHEET

Under **Store Documents at the Post Office?**, mark Yes or No. (Storing documents at the post office is recommended for permanent document storage).

To define a document storage area, you must know its direct access path. For example, a UNC path specifies the absolute location of the document storage folder.

```
\\windows_server\share_name\storage_folder
```

For example:

```
\\win7\c$\docs
```

LIBRARY WORKSHEET

Under **Document Storage Area Path**, specify the direct access path.

Under **Document Storage Area Description**, enter a useful description of the document storage area. (This description is displayed only in the GroupWise Admin console.)

Setting the Start Version Number

You must set the start number for each library to either 0 (zero) or 1. The default is 1. This number identifies the original document.

Version numbers are automatically increased from the number you select. If you select 0, the first version of a document will be 000. If you select 1, the first version will be 001.

LIBRARY WORKSHEET

Under **Start Version Number**, select 0 or 1.

Figuring Maximum Archive Size

Documents created with GroupWise DMS can be archived, depending on their Document Type properties. A document's type determines its disposition, such as archiving or deleting.

When you archive documents, their BLOB files are moved into archive folders. Each library in a document storage area has its own set of archive folders that are automatically created as needed. They are named `ar`*`xxxxxx`* (where *`xxxxxx`* is an incremental integer with leading zeros). A document storage area has the same archive folder structure as the `gwdms` subfolder in the post office.

When a document is archived, GroupWise determines if the document's BLOB file can fit in the current archive folder. If it cannot fit, another archive folder is created and the BLOB is archived there.

An archive set consists of all documents in one archive folder. The Maximum Archive Size property on the Library object establishes in bytes each archive folder's size limit. You should set this to mirror the capacity of your archival medium. It should not be more than your archival medium's capacity.

It is usually better to keep archive sets small in comparison to the size of the backup medium. This lets you back up archive folders often enough to keep your hard disk space from being used up too quickly between backups. For example, if your backup medium has 1 GB capacity, you could limit your archive sets to a maximum archive size of 200 MB.

If your archival system only lets you back up in one pass (in other words, you cannot perform consecutive backups to the medium), the Maximum Archive Size should match the archival medium's capacity.

Some archival mediums require extra space for recording file storage data, such as an index of the files stored to tape. Ten percent is usually sufficient. For example, a tape system with 100 MB capacity means you should set your Maximum Archive Size to 90 MB.

Consult your archival medium documentation for information on setting up an effective backup strategy. Include in your strategy such concepts as multiple archive sets per backup medium, or allowing extra space for the medium's file storage data.

LIBRARY WORKSHEET

Under **Maximum Archive Size**, enter a number (in bytes, with no abbreviations or commas).

Creating a Library

You should already have reviewed "Planning a Library" on page 515 and filled out "Library Worksheet" on page 523. Complete the following tasks to set up a new library:

To create a new library:

1. Ensure that the POA is running for the post office that will own the new library.
2. In the GroupWise Admin console, click **Libraries > New**.
3. Fill in the following fields that you planned for the new post office:

   Name

Post Office

4 Click **OK** to create the new library.

5 In the **Libraries** list, click the name of the new library to configure it:

6 Fill in the following fields as needed:

Display Name
Description
Start Version Number
Maximum Archive Size

7 (Conditional) If you want to store documents outside of the post office folder structure (recommended), click the **Storage Areas** tab.

For instructions on working with document storage areas, see Section 65, "Managing Document Storage Areas in Libraries," on page 525.

8 Click **Save**, then click **Close** to return to the main Admin console window.

9 Continue with Seeing the New Library in the GroupWise Client.

Seeing the New Library in the GroupWise Client

GroupWise client users can immediately see that a new library has been created. They can set it as their default library if desired.

1 In the GroupWise client, click **Tools** > **Options** > **Documents**.

The **Library Configuration** tab should include the new library.

2 (Optional) Select the new library, click **Set as Default** to use the new library as the default location for storing documents and searching for documents.

3 Click **OK**.

4 (Optional) Select the library when you use the Find feature.

Managing Libraries

As your GroupWise DMS system grows and evolves, you might need to perform the following activities:

Managing Library Access

Access to libraries is controlled by the rights users have to the Library object. By default, when a new library is created, all of the following rights are granted:

Public Right	Description
Add	Allows users to add new documents to the library.
Change	Allows users to make changes to existing documents in the library.
Delete	Allows users to delete documents, regardless of who created them or has rights to the documents. However, to be able to delete a document, users must also have rights to locate and modify the document (View and Change rights), in addition to the Delete right.

Public Right	Description
View	By itself, this right allows searching, viewing, or copying documents, but does not permit editing them. Copies can be edited, because a copy is saved as a separate document. Therefore, editing a copy does not affect the original document or any of its versions.
Designate Official Version	Allows any version of a document to be designated as the official version. The official version, which is not necessarily the most recently edited version, is the one located in searches. The official version is usually determined by the creator or author of the document. However, the official version can be designated by the last user to edit the document (if the user has this right). A user also needs the Change right to the document to be able to designate an official version.
Reset In-Use Flag	The In-Use flag protects against data loss by preventing multiple users from concurrently opening the same document. The purpose of the Reset In-Use Flag right is to allow a user or librarian to reset a document's status when the document is in use by someone else or when it is erroneously flagged as in use. In the GroupWise client the document properties Status field displays the current In-Use flag setting for a document. The Status field is automatically set to In Use when a document is opened and reset to Available when a document is closed. There can also be other values, such as Checked Out. A document cannot be checked out when its status is In Use.

There are a variety of reasons for which you might want to restrict certain library rights, including:

- Your libraries are specialized by department and you want to restrict access to sensitive libraries, such as a payroll library.
- Your libraries are distributed across multiple post offices and you want to restrict the scope of user searches to only the libraries they should use, thereby speeding up searches.
- Your libraries are distributed across multiple servers and you want to minimize network traffic.
- You have some users who should have more rights than other users to certain libraries.

To restrict public rights while granting individual rights:

1. In the GroupWise Admin console, browse to and click the name of the library.
2. Click the **Rights** tab.
3. In the **Public Rights** box, deselect the rights that you want to remove from all users.
4. In the **Individual or Group Rights** box, click Add, select the users or groups to grant rights to, then click **OK**.

   If the number is large, you might find it easier to create a group for users who need rights. Then you can select one group rather than multiple users. See Chapter 56, "Creating and Managing Groups," on page 485
5. Above the list, select the rights that you want to grant.
6. Click **Save**, then click **Close** to return to the main Admin console window.

Adding and Training Librarians

When you first create a library, you might for convenience assign yourself as the initial librarian. As library activity increases you can add librarians, and if desired, remove yourself as a librarian.

- "Understanding the Role of the Librarian" on page 520
- "Setting Up a Librarian GroupWise Account (Optional)" on page 522
- "Assigning Librarians" on page 522

Understanding the Role of the Librarian

Keep in mind the following when assigning librarians:

- "Librarian Identity" on page 520
- "Librarian Functions" on page 520
- "Librarian Rights" on page 521

Librarian Identity

Any GroupWise user with access to a library can be a librarian for the library. You can have multiple librarians for a single library. You can also assign a single user as a librarian for multiple libraries. Because being a librarian entails additional functions and rights in the library, you should choose responsible users as librarians.

Librarian Functions

A librarian can perform the following actions:

- Check out a document without a copy.
- Modify the properties of any document in the library.
- Copy documents to another library.
- Delete both documents and properties.
- Reassign document creators and authors to handle orphaned documents
- Reset a document's status (change the In-Use flag).
- View all activity log records of any document in the library.
- Restore document BLOBs from backup.
- Perform mass operations, such as moving, deleting, archiving, and changing properties.
- Perform searches (but not full-text searches) on documents that are not available for searching by regular users.
- Use GroupWise third-party APIs to generate reports on all library documents.

All operations available to a normal user are also available to a librarian, as long as the security requirement discussed under "Librarian Rights" on page 521 is not compromised. The intention is that librarians can modify their own documents and document properties.

All actions taken by a librarian are written to a document's activity log.

Unless the librarian's own GroupWise user name is in the **Author** or **Security** fields, a librarian cannot perform the following functions:

- Open a document

- View a document
- Save a document
- Check out a document with a copy

To help new librarians get started, you should explain these librarian functions to them. You can also refer new librarians to the “librarian users” topic in the GroupWise client help.

Librarian Rights

In addition to the six public rights, libraries also have a Manage right. When you grant the Manage right to a GroupWise user, you designate that user as a librarian. The Manage right gives the librarian full access to the properties of every document in the library. However, the Manage right does *not* grant the librarian direct access to the content of any document.

Because a librarian has full access to document properties, the librarian could add his or her own personal GroupWise user name to the Author or Security field of a document, thus gaining access to the document’s content. However, a high-priority email notification would automatically be sent to the original person listed in the Author field informing him or her of the action by the librarian. Therefore, document privacy is maintained.

The following table lists the various librarian functions, and whether an email notification is sent if the function is performed.

Librarian Function	Notification?
Modify the Author or Security fields	High-priority email to the author
Copy a document	High-priority email to the author
Delete a document	High-priority email to the author
Replace a document with a copy from backup	High-priority email to the author
Perform a mass document operation (copy, move, delete, or archive documents; modify document properties)	Mass operation emails
Reset a document’s status (In-Use flag)	None
Check out a document without a copy	None
View the activity log of any document	None
Generate reports on any documents (using GroupWise third-party APIs)	None

Mass operation notifications do not specify what action was taken by the librarian; they only specify that an action was taken.

The following table lists the document property fields that the librarian has rights to modify, and whether an email notification is sent if the field is modified.

Property Field	Notification?
Subject	No
Author	Yes
Security (sharing list)	Yes
Document Type	No
Version Description	No
Custom Fields	No
File Extension	No
Official Version	No
Current Version	No

If you remove the Manage right from a user, you must manually deselect any rights that the user gained from being made a librarian that the user did not previously have.

Setting Up a Librarian GroupWise Account (Optional)

The Manage right is always in effect for those users who have been assigned as librarians. However, there might be times librarians want to act on their own accord without the possibility of seeing or modifying documents that belong to other users.

To allow users assigned as librarians to act as normal GroupWise users, you could create a single librarian account for a library and have users who need to perform librarian tasks log in using the librarian GroupWise account and password instead of their own.

If users assigned as librarians log in under a librarian GroupWise account, they do not have access to any documents they would normally have access to under their own accounts, except by altering the Author or Security fields.

Assigning Librarians

To add librarians to a library:

1. In the GroupWise Admin console, browse to and click the name of the library.
2. Click the **Rights** tab.
3. In the **Individual or Group Rights** box, select the librarian users, then select **Manage (Librarian)**.
4. Click **Save**, then click **Close** to return to the main Admin console window.

Maintaining Library Databases

The Mailbox/Library Maintenance feature of the GroupWise Admin console offers database maintenance features to keep your library and document databases in good condition. See Chapter 44, "Maintaining Library Databases and Documents," on page 407. It also helps you manage the disk space occupied by library and document databases and document storage areas. See "Reducing the Size of Libraries and Document Storage Areas" on page 416.

When document creators or authors are removed from your GroupWise system, orphaned documents might be left behind. See "Handling Orphaned Documents" on page 531.

To supplement your library maintenance procedures, you should back up your libraries and documents regularly. See "Backing Up a Library and Its Documents" on page 422.

Deleting a Library

You should not delete a library until you ensure that all documents still in the library are no longer needed.

1 In the GroupWise Admin console, click **Libraries**.

2 Select the library to delete, then click **Delete**.

All document storage areas and documents are deleted along with the library.

3 Click **OK** to close the Libraries page and complete the deletion of the library.

Library Worksheet

For instructions on how to use this worksheet, see "Planning a Library" on page 515.

Item	Value for Your GroupWise System	Explanation
Library Name		"Choosing the Library Name" on page 515.
Post Office		"Selecting the Post Office That the Library Will Belong To" on page 515.
Display Name		"Choosing the Library Name" on page 515.
Library Description		"Choosing the Library Name" on page 515.
Start Version Number		"Setting the Start Version Number" on page 516.
Maximum Archive Size		"Figuring Maximum Archive Size" on page 517.
Store Documents at the Post Office? ◆ No ◆ Yes		"Deciding Where to Store Documents" on page 516.
Document Storage Area		"Deciding Where to Store Documents" on page 516.
Document Storage Area Path		"Deciding Where to Store Documents" on page 516.

65 Managing Document Storage Areas in Libraries

For a review, see “Document Storage Areas” on page 513 and “Deciding Where to Store Documents” on page 516.

Typically, the initial document storage area for a library is set up when the library is created. Thereafter, you can create additional document storage areas as the library grows. You can move a document storage area to a location where more storage is available. You can delete a document storage area if it is no longer used.

Adding a Document Storage Area

To help you plan where to create the new document storage area, see “Deciding Where to Store Documents” on page 516.

To create a new document storage area for a library:

1. In the GroupWise Admin console, browse to and click the name of the library.
2. Click the **Storage Areas** tab.

   Existing document storage areas are listed.
3. (Conditional) Deselect **Store documents at post office**.
4. Click **Add** to create a new document storage area.
5. Provide a description for the document storage area.
6. Specify the path to the folder where you want to create the document storage area.

   If the folder does not exist, it will be created as the document storage area is set up.

   If the location is on a remote Windows server:

   6a Specify the remote location as a UNC path.

   6b Configure the POA service to run as This Account on the Windows server with administrator rights to access the remote location.

   6c (Conditional) If the remote location requires different credentials from those in use by the POA service, specify the user name and password for the remote location on the Post Office **Settings** tab.
7. Click **OK** to create the new document storage area and add it to the list of storage areas for the library.
8. In the **Storage Areas** list, select the new document storage area to enable it as an active document storage area.
9. (Conditional) If you want to stop storing documents in the previous document storage area, deselect it in the **Storage Areas** list.
10. Click **Save**, then click **Close** to return to the main Admin console window.

Deleting a Document Storage Area

When you delete a document storage area, any documents in the document storage area are moved to other valid document storage areas for the library. If you want to move documents to a specific location before deleting the document storage area, see "Managing Groups of Documents" on page 527.

To delete a document storage area:

1. In the GroupWise Admin console, browse to and click the name of the library.
2. Click the **Storage Areas** tab.
3. Select a document storage area, then click **Remove**.
4. Click **Save**, then click **Close** to return to the main Admin console window.

If the above steps are not successful in deleting a document storage area, perhaps because one or more documents were in use during the deletion process, you can use the Analyze/Fix Library action of Mailbox/Library Maintenance, with the **Remove Deleted Storage Areas** and **Move Documents First** options selected, to finish cleaning up the deleted document storage area. For more information, see Chapter 44, "Maintaining Library Databases and Documents," on page 407.

66 Creating and Managing Documents

GroupWise Document Management Services (DMS) lets GroupWise client users create documents, save them, then easily locate a specific document later without knowing the application, a specific document name, or the document's physical location.GroupWise client users can create, share, locate, edit, view, and check out documents that are created under the management of GroupWise DMS.

Adding Documents to Libraries

After you set up one or more libraries, users can add new documents to any library to which they have rights. They can also import existing documents into the GroupWise DMS system.

Creating New Documents in the GroupWise Client

1. Click **File** > **New** > **Document**.
2. Select the program you want to use to create the document, select the library where you want to store the document, then click **OK**.
3. In the New Document dialog box, type a brief description of the document.
4. Select **Open Document Now** to open the selected application, then click OK to create the new document.

Importing Existing Documents into the GroupWise DMS System

Some users might have existing documents that they want to manage by adding them to a GroupWise library.

To import documents using the GroupWise client:

1. Click **File** > **Import/Export > Import Documents.**
2. Click **Add Individual Documents**, browse to and select the documents to add, then click **OK**.

   or

   Click **Add Entire Directory**, browse to and select a folder containing documents to import, then click **OK**.

Managing Groups of Documents

As users add documents and your GroupWise DMS system grows, your librarians might need to assist users in managing large groups of documents. If you have not yet assigned librarians to your GroupWise libraries, see "Adding and Training Librarians" on page 520.

To manage large groups of documents in the GroupWise client:

1. Ensure that you are in Online mode.

   The Mass Document Operations feature is not available in Caching mode or Remote mode.
2. Click **Tools** > **Mass Document Operations**.
3. Select the operation to perform on the group of documents:
   - Change properties
   - Move
   - Delete
   - Change sharing
   - Copy
4. Select the method for identifying the group of documents to perform the operation on:
   - Use Find/Advanced Find to select documents
   - Use Find by Example to select documents
   - Use currently selected documents
   - Use documents listed in a file.

Indexing Documents in Libraries

Documents stored in GroupWise libraries need to be indexed so users can locate documents using the Find feature in the GroupWise client. Your organization might need dedicated indexing to minimize performance degradation and network congestion. You might also need dedicated indexing so users can have prompt access to newly created documents.

- "Understanding DMS Indexing" on page 528

Understanding DMS Indexing

Before determining if you will need dedicated indexing, you should have a basic understanding of how indexing works in GroupWise.

- "Index Storage" on page 528
- "Index Content" on page 529
- "Indexing Performed by the POA" on page 529
- "Indexing Cycle" on page 529

Index Storage

When documents are indexed, the information is stored in QuickFinder indexes, which are located in a library's `index` subfolder. A library's QuickFinder index is partitioned into ten *`.idx` files. Additionally, temporary *`.inc` (incremental) files are created that contain each day's new index information. The *`.inc` files are combined once per day into the *`.idx` files (usually at midnight).

In a system with multiple libraries, each library has its own set of QuickFinder index files. Depending on how many libraries belong to a post office, and how many post offices with libraries are in your GroupWise system, there can be many sets of QuickFinder index files.

Index Content

Indexing can include a document's full text (depending on its document type), and always includes the document's property sheet information (subject, author, version descriptions, and so on). Both newly edited and newly created documents are indexed, which means indexing volume is determined by how many existing documents are edited as well as how many new documents are created.

Newly-created documents must be indexed before users can search for them. In setting up your indexing strategy, you must know how quickly users will need access to newly-created documents.

The standard search is limited to the QuickFinder indexes in the user's default library. But users can choose to search for documents in other libraries to which they have access.

Indexing Performed by the POA

Indexing is among the many functions of the POA. To learn more about POA functions, see "Role of the Post Office Agent" on page 139.

You can configure the POA for a post office to meet varying indexing needs. See "Configuring Indexing" on page 177. On a server with adequate memory and disk space, the POA can keep up with indexing demands in a typical post office.

If you want to set up an additional POA specifically to handle indexing, see "Creating a New POA in the GroupWise Admin Console" on page 144. You can temporarily use multiple indexing POAs for importing documents to speed up importing time.

Indexing Cycle

The frequency of indexing is determined by the POA QuickFinder Interval setting. The default is once every 24 hours at 8:00 p.m. You can specify the QuickFinder Interval setting in one-hour increments. For example, a setting of 1 would allow users to find documents created as recently as an hour ago. You can set the QuickFinder Interval to 0 (zero) for continuous indexing, but this might impact other POA functioning.

Managing Documents in Libraries

As more and more documents are added to your GroupWise libraries, you must manage the disk space occupied by libraries and respond to various changes in your GroupWise system.

See also Section 65, "Managing Document Storage Areas in Libraries," on page 525.

Archiving and Deleting Documents

You can use the Mailbox/Library Maintenance feature in the GroupWise Admin console to archive and delete documents on demand. See "Reducing the Size of Libraries and Document Storage Areas" on page 416.

You can also configure the POA to archive and delete documents on a regular schedule. See "Scheduling Disk Space Management" on page 156.

Backing Up and Restoring Archived Documents

When documents are archived, they are physically moved to a folder in the post office, where disk space can be limited. You should move archived documents to your backup medium regularly.

- "Moving Archived Documents to Backup" on page 530
- "Restoring Archived Documents" on page 530

Moving Archived Documents to Backup

When documents are archived, they are placed in automatically created archive folders. Each library has a set of archive folders. For example, `gwdms` (GroupWise Document Management Services) is one of the post office's folders. The library folders exist under it, named `lib0001-`*`ff`*. Under each library folder is an archive folder, under which are the sequentially-numbered archival folders, named `ar`*`nnnnnn`* (where *nnnnnn* is an integer with leading zeros). Each `ar`*`nnnnnn`* folder is an archive set.

To move archived documents to backup:

1. Ensure that you have a backup medium operating with your system.
2. Ensure that you have already archived documents that have reached their expiration dates. Documents that have not been archived cannot be removed to a backup medium.
3. Start the software for your backup medium.
4. When the backup software asks for the location of your archive files, give the full path.

   Example:

   ```
   j:\post_office\gwdms\lib0\archive\ar000001
   ```

Restoring Archived Documents

When a user tries to access a document that has been archived, one of two things happens:

- If the document is in the post office archive set, and has not yet been physically moved from the archive location, the document opens normally. The user does not realize it was archived. The document is unarchived from the archive set at that time; that is, it is moved back to the library document folder from which it was archived. It is also given a new archive date according to the document type.
- The user sees a message indicating the document cannot be opened. In this case, the archive set containing the document has been physically moved to a backup medium. Therefore, the document cannot be automatically unarchived. In this case, the user might contact you, asking you to locate or recover the document. You can restore either the document's BLOB or the archive set that contains the BLOB. After the document is restored to its archive folder, the user will be able to open the document normally.

To restore archived documents from a backup medium:

1. Obtain the Document Number for the document the user was trying to access.
2. In the GroupWise client, click **Tools > Find**.
3. Specify the Document Number, then click **OK**.
4. Right-click the document in the **Find Results** listing, then click **Properties > Version**.
5. Note the archive folder in the path listed in the **Current Location** field.

   The subfolder listed after the ..`\archive` folder is the archive set containing the document, for example, `\ar000001`.

6 If you have the ability to recover individual files from your backup medium, also note the BLOB file name listed in the **Current Filename** field.

7 Determine where you backed up the archive set, then copy either the archive set or the individual BLOB file to the archive folder specified in the Current Location field that you noted earlier.

8 You can now notify the user that the requested document is available.

9 When you are sure the user has opened the document (causing it to be unarchived), you should delete any files remaining in that archive folder because you have already backed them up.

Handling Orphaned Documents

If you remove public rights for a library, some documents might become inaccessible. For example, if a user who has been denied access to the library is the only user who had access to certain documents, those documents become orphaned. No other user can access or search for those orphaned documents. This is because document security is controlled by the user listed in the **Author** and **Creator** fields in the document's properties. In other words, if the author or creator no longer has access to a document, neither does anyone else.

However, orphaned documents can be reassigned to another author so that someone can access them again. This can be done in one of two ways:

- In the GroupWise Admin console, the Analyze/Fix Library action in Mailbox/Library Maintenance can reassign orphaned documents to a specified user. Then, the new user has access to all orphaned documents in that library. For more information, see Chapter 44, "Maintaining Library Databases and Documents," on page 407.
- A librarian has the ability to alter the Author field of documents. Therefore, a librarian can replace the previous user's GroupWise user name with his or her own user name. In doing so, the librarian becomes the new author of the document. This can also be done as a mass operation for multiple documents with varying GroupWise user names in the Author field. For more information, see "Adding and Training Librarians" on page 520.

XIV Client

67 Using GroupWise Client Custom Installation Options

You can customize the installation of the GroupWise client for use with ZENworks or other software distribution system by using GWTuner. Along with customizing the installation, you can extract the GroupWise client software to deploy to your workstations or to make it available on your web server.

Using GWTuner

The GWTuner utility allows you to customize your GroupWise MSI installation. GWTuner creates an MST transform file named `groupwise.mst`, which you can use when performing an MSI install with ZENworks or other MSI install software.The GWTuner provides the following options for customizing the installation of the GroupWise client:

Languages	You can install the GroupWise client in one or more languages. For a list of available languages, see"GroupWise User Languages" on page 85.
Internet Browser Mail Integration	By default, GroupWise is enabled to be the default email application when you click a `mailto` link in your web browser or use the `Mail` command in your web browser.
Program Folder	By default, the Setup program creates a `Micro Focus\GroupWise` program folder. You can use a different folder as needed.
Add GroupWise to the Desktop	By default, the Setup program creates a GroupWise icon on your Windows desktop.
Add GroupWise to Quick Launch	By default, the Setup program adds a GroupWise icon to the Windows Quick Launch bar
Add Notify to the Startup Folder	By default, the Setup program does not add Notify to the Windows Startup folder. If you want to start Notify automatically, but if you do not want to use the Windows Startup folder, you can click **Tools > Options > Environment**, then select **Launch Notify at startup** in the GroupWise client to have GroupWise automatically start Notify.
Add Icons to the Start Menu	By default, the Setup program adds GroupWise to the Windows Start Menu and includes a list of GroupWise tasks that can be performed directly from the Start Menu.

To create the `groupwise.mst` file:

1 On the Windows server, ensure that you have write access to the following folder in the downloaded *GroupWise 18* software image:

groupwise_software_image\admin\utility\tools

NOTE: The GWTuner utility is available in both the Windows and Linux *GroupWise 18* software image.

2 Run the following program:

groupwise_software_image\admin\utility\tools\gwtuner.exe

3 When prompted for the client directory, browse to the following folder, then click **Next**.

groupwise_software_image\client

4 In the **Install path** field, specify where you want to install the GroupWise client software on users' workstations.

   The typical location varies depending on the architecture of the workstations:

32-bit architecture:	`C:\Program Files\Micro Focus\GroupWise`
64-bit architecture:	`C:\Program Files (x86)\Micro Focus\GroupWise`

   If all of the workstations in your environment have the same architecture, specify the appropriate location for that architecture. If you have both 32-bit and 64-bit workstations in your environment, you can specify either path in GWTuner. In ZENworks Configuration Management, you will create a separate launch action for each architecture.

5 Select GroupWise client installation options as needed.

   For information about the GroupWise client installation options, see "Using GroupWise Client Custom Installation Options" in the *GroupWise 18 Administration Guide*.

6 Select all the languages that you want to install on users' workstations, then click **Next**.

7 Select the default GroupWise client startup language, then click **Finish**.

8 Click **OK** to exit GWTuner.

   The following MST transform file is created in the downloaded *GroupWise 18* software image:

   groupwise_software_image\client\win32\groupwise.mst

For instructions on installing the GroupWise client using ZENworks, see "Using ZENworks Configuration Management to Distribute the GroupWise Client" on page 592.

Extracting the GroupWise Software

When you run the GroupWise Installation Wizard to install the GroupWise Server component, the GroupWise client software is installed in the following locations:

Linux:	`/opt/novell/groupwise/agents/data/client/setup/win32`
Windows:	`c:\Program Files\Micro Focus\GroupWise Server\agents\data\client\setup\win32`

If you do not want to run the GroupWise Installation Wizard to gain access to these files, you can manually extract the files.

1 Create a temporary folder on the web server for storing the GroupWise software.

   For example, you could name the folder `gw18software`.

2 On Linux, use the following procedure to extract the GroupWise software files:

   2a Change to the folder that you created in Step 1.

   2b Know the path to the `novell-groupwise-server.64bit.rpm` file in the downloaded *GroupWise 18* software image:

   /*groupwise_software_image*/server/linux/x86_64/

   2c Use the following command to extract the GroupWise Server component:

```
rpm2cpio /path/novell-groupwise-server.64bit.rpm | cpio -idmv
```

This creates the folder where the GroupWise software is located:

`/`*`gw18software`*`/agents/data/client/setup/win32`

3 On Windows, use the following procedure to extract the GroupWise software files.

3a Change to the following folder in the downloaded *GroupWise 18* software image:

`\`*`groupwise_software_image`*`\server\win64`

3b Use the following command to extract the GroupWise Server component into the folder that you created in Step 1.

`setup.exe /extract c:\`*`gw18software`*

This creates the folder where the GroupWise client software is located:

`\`*`gw18software`*`\Micro Focus\GroupWise Server\agents\data\client\setup\win32`

68 Setting Up GroupWise Client Modes and Accounts

As a GroupWise administrator, you might need to help users with the various GroupWise modes and account types.

GroupWise Client Modes

GroupWise provides three different ways to run the GroupWise client: Online mode, Caching mode, and Remote mode.

Most GroupWise features are available in all three GroupWise modes, with a few exceptions:

- Subscribing to other users' notifications is not available in Caching mode.
- Subscribing to other users' notifications and Proxy are not available in Remote mode.

Online Mode

When users use Online mode, they are connected to their post office on the network. The user's mailbox displays the messages and information stored in the network mailbox, which is called the Online mailbox. Online mode is connected to the Online mailbox continuously. In Online mode, if the POA shuts down or users lose network connection, they temporarily lose the connection to their mailboxes.

Users should use this mode if they do not have a lot of network traffic, or if they use several different workstations and do not want to download a local mailbox to each one.

Caching Mode

Caching mode stores a copy of a user's Online mailbox, including messages and other information, on the user's local drive. This allows GroupWise to be used whether or not the network or POA is available. Because the user is not connected to the network all the time, this mode cuts down on network traffic and has the best performance. A connection is made automatically to retrieve and send new messages. All updates are performed in the background, so that GroupWise work is not interrupted.

Users should use this mode if they have enough disk space on the local drive to store the Caching mailbox. If users run Caching mode and Remote mode on the same computer, the same local mailbox can be used to minimize disk space usage.

By backing up their Caching mailboxes, users can protect items that might be deleted if the system is set up to automatically clean up items, or if the GroupWise administrator runs an Expire and Reduce.

Several users can set up their Caching mailboxes on a single shared computer.

The default location for a Caching mailbox varies by client platform:

Windows 8:	`c:\Users\`*`user_name`*`\AppData\Roaming\Micro Focus\GroupWise`
Windows 7:	`c:\Users\`*`user_name`*`\AppData\Roaming\Micro Focus\GroupWise`
Windows XP:	`c:\Documents and Settings\`*`user_name`*`\Local Settings\Application Data\Micro Focus\GroupWise`

As a GroupWise administrator, you have some control over what modes GroupWise client users choose to use and how Caching mode worked:

* "Allowing or Forcing Use of Caching Mode" on page 540
* "Downloading the GroupWise Address Book in Caching Mode" on page 541

Allowing or Forcing Use of Caching Mode

As the GroupWise administrator, you can allow or disallow the use of Caching mode, and can also force users to log in to GroupWise in Caching mode.

1. In the GroupWise Admin console, browse to and click the name of the post office.
2. Click **Client Options**.
3. Click the **Environment** tab, then click **Client Access**.
4. Select or deselect **Allow Use of Caching Mode**.
5. Select or deselect **Force Use of Caching Mode**.

   Specify the number of days before Caching mode is enforced. This allows the user to continue using Online mode until the grace period has passed. The grace period begins the first time the user connects to the POA. The setting applies per user per workstation.

   The **Force Caching Mode** setting is not enforced on a workstation that does not have enough disk space for a Caching mailbox. The amount of disk space that is required is the size of the mailbox + 20 MB + 25% of the mailbox size.

   The **Force Caching Mode** setting is also not enforced when a user connects from a shared Windows workstation or terminal server if you configure these workstations to be excluded. You do this by setting a registry key on the Windows workstation. The registry key is in HKEY_LOCAL_MACHINE. Under `Software\\Micro Focus\\GroupWise\\Client`, add a dword value named No Local Store with a value of 1. This prevents the user from creating a Caching or Remote mailbox by using the GroupWise client menus. However, the user can still create a Caching or Remote mailbox by using the startup options /pc, /pr, or /ps.

If you force Caching mode and then restrict Online mailbox size so that users have items in their Caching mailboxes that are no longer available online, you need to ensure that users understand about doing backups. See "Backing Up Email" in the *GroupWise 18 Client User Guide.*

Downloading the GroupWise Address Book in Caching Mode

When users prime their Caching mailboxes, they receive a copy of the GroupWise Address Book. After the initial priming of the Caching mailbox, users can re-download the GroupWise Address Book and their personal address books in Caching mode by clicking **View > Retrieve System Address Book** or **View > Retrieve Personal Address Book** in the GroupWise Address Book. Address books can also be re-downloaded in Caching mode when users click **Tools > Retrieve Entire Mailbox**.

Users can also specify to download the GroupWise Address Book (and any rules they have created) on a regular basis.

1. In Remote or Caching mode, click **Accounts > Account Options**.
2. Select the GroupWise account, then click **Properties > Advanced**.
3. Select **Refresh Address Books and Rules Every __ Days**. By default this is set to 0 days, but it can be changed.

If you configure the POA to generate the GroupWise Address Book regularly, Caching mode users always have a current copy to download.

1. In the GroupWise Admin console, browse to and click the POA.
2. Click the **Maintenance** tab, then locate the **Generate Address Book for Remote** section and ensure it is enabled.

You can choose the time when you want the generation to take place.

If you want to generate the GroupWise Address Book for download more than once a day, you can delete the existing `wprof50.db` file from the `\wpcsout\ofs` subdirectory of each post office. A new downloadable GroupWise Address Book is generated automatically for users on each post office.

Remote Mode

Remote mode is familiar to GroupWise users who use Hit the Road. Similar to Caching mode, a copy of the Online mailbox, or the portion of the mailbox that users specify, is stored on the local drive. Users can periodically retrieve and send messages with the type of connection they specify (modem, network, or TCP/IP). Users can restrict what is retrieved, such as only new messages or only message subject lines.

As a GroupWise administrator, you can allow or disallow the use of Remote mode for client users.

1. In the GroupWise Admin console, browse to and click the name of the post office.
2. Click **Client Options**.
3. Click the **Environment** tab, then click **Client Access**.
4. Select or deselect **Allow Use of Remote Mode**.

The following topics explain the capabilities users have when they are allowed to use Remote mode.

- "Hit the Road" on page 542
- "Remote Properties" on page 542
- "Remote Mode Connections" on page 542

Hit the Road

Users can use **Hit the Road** on the **Tools** menu (or the startup option from Online mode to Remote mode) to create, set up, or update the Remote mailbox. A copy of the mailbox is created on the user's local drive, and any current connections are detected and set up. If users have already used Caching mode, the local mailbox has already been created. Users can also use **Hit the Road** to create setup files on a removable storage device (for example, a flash drive) to set up their Remote mailbox on a computer that is not connected to the network. Several users can set up their Remote mailboxes on a single shared computer.

Hit the Road creates a TCP/IP connection to the Online mailbox. GroupWise can then use this connection to connect to the GroupWise system when running in Remote mode. For example, a network connection lets users of docked laptops run GroupWise in Remote mode and connect to the GroupWise system through the network connection rather than a modem connection.

To use **Hit the Road**:

1. In the GroupWise client, click **Tools > Hit the Road**.
2. Follow the prompts to create the Remote mailbox on the computer or on a removable storage device.

If **Hit the Road** created the user's Remote mailbox on a removable storage device, the user needs to install the Remote mailbox on the computer that will be running in Remote mode.

1. Insert the removable storage device containing the Remote mailbox into the computer.
2. Run `setup.exe` on the removable storage device.

   Follow the prompts. The Setup program creates a Remote mailbox and copies the required files to the computer's hard drive.

Remote Properties

Users can change the way Remote mode is set up, including the connection, time zone, signature, and so on, by using **Account Options** on the **Accounts** menu. Remote is listed as an account.

By default, if an item is deleted from the Remote mailbox, the item is deleted from the Online mailbox the next time a connection is made. Deletion options in Remote Properties can be changed so that an item deleted from the Remote mailbox stays in the Online mailbox or vice versa.

Remote Mode Connections

- "Setting Up a Network Connection" on page 542
- "Setting Up a TCP/IP Connection" on page 543

Setting Up a Network Connection

While running in Remote mode, GroupWise can connect to the user's Online mailbox using a network connection. A network connection is useful for laptop users connecting to the network through a docking station, or for remote users connecting through a modem using remote node software.

To create a network connection:

1. In the GroupWise client, log in or change to Remote mode.
2. Click **Accounts > Send/Retrieve > GroupWise Options**.
3. Click **Network > OK**.

4 Type a descriptive name for the network connection in the **Connection Name** box.

5 Type the path to any post office directory in the master GroupWise system.

Users can connect to their own post offices or to any post office in the master GroupWise system to access their Online mailboxes.

6 Click a disconnect method:

Method	Description
When All Updates Are Received	Disconnects after requests are sent and after all responses to the requests are received (or disconnects automatically when the time allowed by the gateway has expired).
Do Not Wait for Responses	Disconnects immediately after requests are sent and pending responses are received. Pending responses are responses to other requests that are waiting to be downloaded to you.
Manually	Lets you manually control when to disconnect (or disconnects automatically when the time allowed by the gateway has expired).

7 Click **OK**.

8 Select the connection you want, then click **Select**.

9 Select the location you are connecting from in the **Connecting From** box. If none are listed, use the **Default Location** option.

If you need to create a new location, click the **Connect From** button. This is useful for laptop users who are calling into the GroupWise system from different geographic locations.

10 Click **OK**, then click **Close**.

Setting Up a TCP/IP Connection

A TCP/IP connection enables GroupWise, while running in Remote mode, to connect to the GroupWise system through a network connection using TCP/IP. A TCP/IP connection can be made through a network connection, such as a laptop connecting to the network through its docking station, or through a modem using remote node software.

To create a TCP/IP connection:

1 In the client, log in or change to Remote mode.

2 Click **Accounts > Account Options**, then double-click the Remote account.

3 Click **Connection > Connect To > New > TCP/IP > OK**.

4 Type a descriptive name for the TCP/IP connection.

5 Type the IP address or the DNS name.

6 Type the IP port for this address.

7 Click a disconnect method:

Method	Description
When All Updates Are Received	Disconnects after requests are sent and after all responses to the requests are received (or disconnects automatically when the time allowed by the gateway has expired).

Method	Description
Do Not Wait for Responses	Disconnects immediately after requests are sent and pending responses are received. Pending responses are responses to other requests that are waiting to be downloaded to you.
Manually	Lets you manually control when to disconnect (or disconnects automatically when the time allowed by the gateway has expired).

8 Click **OK**.

9 Select the connection you want, then click **Select**.

10 Select the location you are connecting from in the **Connecting From** box. If none are listed, use the **Default Location** option.

If you need to create a new location, click the **Connect From** button. This is useful for laptop users who are calling into the GroupWise system from different geographic locations.

11 Click **OK**, then click **Close**.

Email Accounts

Accounts Menu

In addition to the Remote account, users can access and configure POP3 and IMAP4 Internet email accounts and NNTP News accounts from the **Accounts** menu. While the user is in Remote and Caching mode, POP3, IMAP4, and NNTP accounts are accessed without needing to connect to the GroupWise system. If the GroupWise Administrator enables it, users can also access and configure their POP3, IMAP4, and NNTP accounts from the **Accounts** menu in Online mode.

Enabling POP3, IMAP4, and NNTP Account Access in Online Mode

By default, POP3, IMAP4, and NNTP accounts can be added, configured, and accessed by users in Remote and Caching mode only. Account items and information are not accessible in Online mode, nor can items and information be uploaded to the Online mailbox unless the GroupWise administrator enables it.

To enable POP3, IMAP4, and NNTP account access for clients in Online mode for an entire post office:

1. In the GroupWise Admin console, browse to and click the name of the post office.
2. Click **Client Options**.
3. Click the **Environment** tab, then click **General**.
4. Select **Allow Use of News (NNTP) Accounts in the Online Mailbox.**
5. Select **Allow Use of POP and IMAP Accounts in the Online Mailbox**.
6. Click **OK**.

69 Setting Defaults for the GroupWise Client Options

The GroupWise client includes options (preferences) that can be set by individual users. As a GroupWise administrator, you can determine the default settings for many of the options. If you do not want users to change the default settings that you have established, you can lock the settings.

Client Options Summary

Default settings can be established at the user level, the post office level, or the domain level. User settings override post office settings, and post office settings override domain settings.

If you set a lock on an option at a higher level, the higher level then overrides the lower-level setting. When you change an option and lock it, the new setting is immediately put into effect.

1. In the GroupWise Admin console, browse to and click a domain, post office, or user.
2. Click **Client Options**.

The client options table in this section summarizes all client options and provides links to descriptions of the options. For more detailed instructions, see Chapter 69, “Setting Defaults for the GroupWise Client Options,” on page 545.

- Environment
- Send
- Calendar
- Security
- Integrations
- Documents

Client Options Type	Client Options Tab	Client Options
Environment Click a Domain, Post Office, or User, then click **Client Options > Environment**	**General**	Refresh Interval Allow Shared Folder Creation Allow Shared Address Book Creation Check Spelling As You Type Check Spelling Before Send Show Messenger Presence Allow Use of News (NNTP) Accounts in the Online Mailbox Allow Use of POP and IMAP Accounts in the Online Mailbox IMAP Copy Results in a GroupWise Move Allow Searches of Non-Indexed Attachments

Client Options Type	Client Options Tab	Client Options
	Address Book	Allow Creation of User Defined Fields in the Personal Address Book Enable Auto-Saving Save Addresses of Items That Are Received From external sources (Internet) From internal sources Save Addresses of Items That Are Sent To external sources (Internet) To internal sources
	Appearance	Scheme Settings Schemes Default GroupWise Classic Simplified Custom Display Main Menu Display Nav Bar Display Main Toolbar Use GroupWise Color Schemes Display Folder List Favorites Folder List Simple Folder List Full Folder List Long Folder List Display QuickViewer QuickViewer at Bottom QuickViewer at Right
	Client Access	Client Licensing Full License Mailboxes Limited License Mailboxes Client Login Mode Allow Use of Remote Mode Allow Use of Caching Mode Force Caching Mode after __ Days

Client Options Type	Client Options Tab	Client Options
	Cleanup	Force Synchronization of Cleanup Options to Caching/ Remote Allow User to Protect Items from Auto Cleanup Mail and Phone Manual Delete and Archive Auto-Delete After Auto-Archive After Appointment, Task, and Note Manual Delete and Archive Auto-Delete After Auto-Archive After Empty Trash Manual Automatic After Maintenance Do Not Purge Items Until They Are Backed Up Prompt before Purging Perform Maintenance Purges on Caching/Remote
	File Location	Archive Directory Custom Views
	Junk Mail	Junk Mail Handling Enable Junk Mail Using Junk Mail Lists Enable Junk Mail Using Personal Address Book Enable Junk Calendaring Using Personal Address Book Auto-Delete After Enable Blocked Mail Using Block Mail Lists
	Reply Format	Plain Text Reply Format HTML Reply Format
	Views	View Options Read Next After Accept, Decline, or Delete Open New View after Send Disable HTML View Read Views Default Plain Text HTML Allowed Plain Text HTML Compose Views Default Plain Text HTML Allowed Plain Text HTML

Client Options Type	Client Options Tab	Client Options
	Client Auto-Update	Enable Client Auto-Update Auto-Update URL Force Update Grace Logins Prompt until Updated
Send Click a Domain, Post Office, or User, then click **Client Options > Send**	**Send Options**	General Classification Normal, Proprietary, Confidential, Secret, Top Secret, For Your Eyes Only MIME Encoding Wildcard Addressing Maximum Recipients Allowed Restricted Attachment Extensions Allow Use of “Reply to All” in Rules Allow Use of “Internet Mail” Tracking Notify Recipients Convert Attachments Allow Reply Rules to Loop Expiration Date Delay Delivery Priority High, Standard, Low Reply Requested When Convenient, Within __ Days
	Mail	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification When Opened/Deleted None, Mail Receipt, Notify, Notify and Mail
	Appointment	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification When Opened/Accepted/Deleted None, Mail Receipt, Notify, Notify and Mail
	Task	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification When Opened/Accepted/Completed/Deleted None, Mail Receipt, Notify, Notify and Mail

Client Options Type	Client Options Tab	Client Options
	Note	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification When Opened/Deleted None, Mail Receipt, Notify, Notify and Mail
	Disk Space Management	User Limits Mailbox Size Limit Threshold for Warning Users Maximum Send Message Size Limits Apply to Cache Notify the Administrator When Threshold Limit Is Exceeded Notify the Administrator When Size Limit Is Exceeded
	Global Signature	Global Signature Apply Signature to All Messages Apply Signature to External Messages Only
	Security	Conceal Subject Require Password to Complete Routed Item Secure Items Options Do Not Allow Use of S/MIME URL for Certificate Download Sign Digitally Encrypt for Recipients Encryption Algorithm Encryption Key Size
Calendar Click a Domain, Post Office, or User, then click **Client Options > Calendar**	General	Month Display Option First of Week Highlight Day Show Week Number Appointment Options Include Myself on New Appointments Display Appointment Length As Duration, End Date and Time Default Length Alarm Options Set Alarm When Accepted Default Alarm Time Work Schedule Start/End Time Work Days

Client Options Type	Client Options Tab	Client Options
	Web Calendar	Web Calendar Publishing Host Enable Calendar Publishing Enable Rules to Move Items to a Published Calendar Enable Publish Free/Busy Search Enable Subscribe to Calendar
	Busy Search	Appointment Length Range and Time to Search Work Schedule
Security Click a Domain, Post Office, or User, then click **Client Options > Security**	Password	Password Clear User's Password Allow eDirectory Authentication Instead of Password Enable Single Sign-On Use Collaboration Single Sign-On (CASA)
	Notify	Check for Mail Every
Integrations Click a Domain, Post Office, or User, then click **Client Options > Integrations**	Micro Focus Vibe	Enable Micro Focus Vibe Micro Focus Vibe URL
	Retention	Enable Message Retention Service
	Tutorial	Training and Tutorial URL
Documents Click a Domain, Post Office, or User, then click **Client Options > Documents**	Library Configuration	Default Library

Setting Client Options

Default settings can be established at the user level, the post office level, or the domain level. User settings override post office settings, and post office settings override domain settings.

If you set a lock on an option at a higher level, the higher level then overrides the lower-level setting. When you change an option and lock it, the new setting is immediately put into effect.

To modify the default settings for the GroupWise client:

1. In the GroupWise Admin console, browse to and click the name of a domain if you want to modify the settings for all users in the domain.

   or

   Browse to and click the name of a post office object if you want to modify the settings for all users in the post office.

   or

Browse to and click a user if you want to modify settings for the individual user. To change the same settings for multiple users, select multiple objects.

2 Click **Client Options** to display the GroupWise Client Options dialog box.

3 To set the Environment options, click **Environment**, then continue with "Modifying Environment Options" on page 551.

or

To set the Send options, click **Send**, then skip to "Modifying Send Options" on page 563.

or

To set the Calendar options, click **Calendar**, then skip to "Modifying Calendar Options" on page 573.

or

To set the Security options, click **Security**, then skip to "Modifying Security Options" on page 577.

orTo set the Integrations options, click **Integrations**, then skip to "Modifying Integrations Options" on page 579.or

To set the Documents options, click **Documents**, then skip to "Modifying Documents Options" on page 581.

Modifying Environment Options

1 In the GroupWise Admin console, display the Client Options **Environment** tab.

For instructions, see Chapter 69, "Setting Defaults for the GroupWise Client Options," on page 545.

2 Click the tab that contains the options that you want to change:

"Environment Options: General" on page 552
"Environment Options: Address Book" on page 553
"Environment Options: Appearance" on page 553
"Environment Options: Client Access" on page 554
"Environment Options: Cleanup" on page 555
"Environment Options: File Location" on page 557
"Environment Options: Junk Mail" on page 558
"Environment Options: Reply Format" on page 560
"Environment Options: Views" on page 561
"Environment Options: Client Auto-Update" on page 562

3 If you want to prevent users from changing an option's setting, click the lock button next to it.

After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.

4 If you want to return all the options on a tab to their default settings, click **Restore Default Settings**.

5 When you are finished, click **OK** to save your changes.

Environment Options: General

The **General** options determine such settings as the refresh interval for new messages, whether users can create shared folders and address books, and which types of accounts can be used in Online mode.

Refresh Interval

Determines how often the GroupWise client message lists are updated to reflect new message status. The default is 1 minute.

Allow Shared Folder Creation

Enables users to share folders with other users. By default, this option is enabled.

Allow Shared Address Book Creation

Enables users to share address books with other users. By default, this option is enabled.

Check Spelling As You Type

Automatically spell checks as text is typed. By default, this option is enabled.

Check Spelling Before Send

Automatically spell checks the message text of each item before the item is sent. By default, this option is disabled.

Show Messenger Presence

Displays Messenger presence information in the GroupWise client. Messenger presence enables users to easily choose instant messaging as an alternative to email. Messenger presence icons appear in the **From** field of a received message, in the Quick Info for users specified in the **To**, **CC**, and **BC** fields of a new message, and in the Quick Info for users in the GroupWise Address Book. Messenger presence is enabled by default.

Allow Use of POP and IMAP Accounts in the Online Mailbox

Select this option to enable users to access POP and IMAP accounts while using the GroupWise client in Online mode.

By default, this option is disabled. If you enable this option, an **Accounts** menu is added to the GroupWise client, allowing users to add POP and IMAP accounts to GroupWise, set account properties, and send and retrieve items from their POP and IMAP accounts. In addition, users are allowed to upload POP and IMAP items from the Remote mailbox to the Online mailbox.

Allow Use of News (NNTP) Accounts in the Online Mailbox

Select this option to enable users to set up newsgroup (NNTP) accounts while using the GroupWise client in Online mode.

IMAP Copy Results in a GroupWise Move

By default, when you move an item from one folder to another in an IMAP email client, the IMAP email client creates a copy of the item in the new location and marks the original item for deletion. The IMAP email client might display the original item with strikeout markup, to indicate that it will be

deleted according to the cleanup schedule you have selected. Or the IMAP email client might hide such items until they are automatically cleaned up. When this IMAP behavior synchronizes to your GroupWise mailbox, GroupWise by default displays the original items with the strikeout markup, and you might have been manually deleting those items from your GroupWise mailbox. Select this option so that items with strikeout markup no longer display in GroupWise.

Allow Searches of Non-Indexed Attachments

By default, a client Find will search all attachments (including those which require DVA conversion). If this option is set to Enabled if POA resources are available, then the search will only look through all attachments if the POA has al least 20% of the C/S threads available. You can also set this to be disabled if you do not want searches to be able to look through non-indexed attachments.

Environment Options: Address Book

The Address Book options enable you to control how users configure the functioning of their Frequent Contacts address books. You can also control whether users can create custom columns in their personal address books.

Allow Creation of User Defined Fields in the Personal Address Book

Select this option to allow users to create custom columns in their personal address books.

Enable Auto-Saving

By default, email addresses of those to whom users send messages are automatically added to their Frequent Contacts address books. Users can also choose to automatically save email addresses of those from whom they receive messages. Deselect this option if you do not want email addresses to be automatically saved.

- **Save Addresses of Items That Are Received:** Select this option to allow users to automatically add external and internal email address from items that they receive to their Frequent Contacts address books. If desired, you can restrict users to collecting email addresses only if the user’s name or email address appears in the **To** field, as opposed to the **CC** or **BC** fields.
- **Save Addresses of Items That Are Sent:** Select this option to allow users to automatically add external and internal email address from items that they send to their Frequent Contacts address books.

Environment Options: Appearance

The **Appearance** options determines the appearance of the GroupWise client.

Schemes

There are four available schemes that determine how the GroupWise Client appears.

- **Default:** The Default scheme displays the Nav Bar, Full Folder List, the Main Menu, and two columns with panels.
- **GroupWise Classic:** The GroupWise Classic scheme has the Folder List, Main Toolbar, and Item List, displaying in the old GroupWise 6.5 colors.
- **Simplified:** The Simplified scheme has the Nav Bar, Simple Folder List, and two columns with panels.
- **Custom:** The Custom scheme allows you to set the appearance settings however you like. If you edit one of the predefined schemes, those settings become your Custom scheme.

Scheme Settings

You can also control individual appearance settings for the GroupWise client.

- **Display Main Menu:** Displays the menu at the top of the window in the GroupWise client.
- **Display Nav Bar:** Displays the Nav Bar at the top of the window in the GroupWise client.
- **Display Main Toolbar:** Displays the toolbar underneath the Nav bar in the GroupWise client.
- **GroupWise Color Scheme:** Overrides any operating system color schemes for the GroupWise client.
- **Display Folder List:** Displays the Folder List on the left side of the window in the GroupWise client. You can select from a Favorites Folder List, Simple Folder List, Full Folder List, or Long Folder List. For descriptions, see "Customizing Individual GroupWise Appearance Settings" in the *GroupWise 18 Client User Guide*.
- **Display QuickViewer:** Displays the QuickViewer in the GroupWise client. You can select to display the QuickViewer on the right side or at the bottom.

Environment Options: Client Access

The **Client Access** options allow you to apply a license type (full or limited) to users' mailboxes and enable or disable the Remote and Caching modes in the GroupWise client.

Client Licensing

GroupWise offers two types of mailbox licenses: Full Licenses and Limited Licenses.

You can use this option to specify the type of mailbox license that you want applied to users' mailboxes. This enables you to support the type of GroupWise mailbox licenses you purchase. For example, if you only purchased Limited License mailboxes for users on a specific post office, you can mark all mailboxes on that post office as being Limited License mailboxes.

For licensing details, see "Auditing Mailbox License Usage in the Post Office" on page 127.

Client Login Mode

Choose from the following settings to determine which login modes are available to GroupWise users when using the GroupWise client. These settings apply only if you selected **Full License Mailboxes** for the client licensing.

- **Allow Use of Remote Mode:** Select this option to enable users to log in with GroupWise in Remote mode. With Remote mode, the GroupWise client uses a Remote mailbox on the user's local drive. The user must initiate a connection (modem, direct, or TCP/IP) to send or retrieve items from the GroupWise system. For more information about Remote mode, see "Remote Mode" on page 541. By default, this option is enabled.
- **Allow Use of Caching Mode:** Select this option to enable users to log in with GroupWise in Caching mode. With Caching mode, the GroupWise client uses a Caching mailbox on the user's local drive (this can be the same mailbox as the Remote mailbox). The GroupWise client periodically initiates a connection with the GroupWise system to send and receive items. For more information about Caching mode, see "Caching Mode" on page 539. By default, this option is enabled.

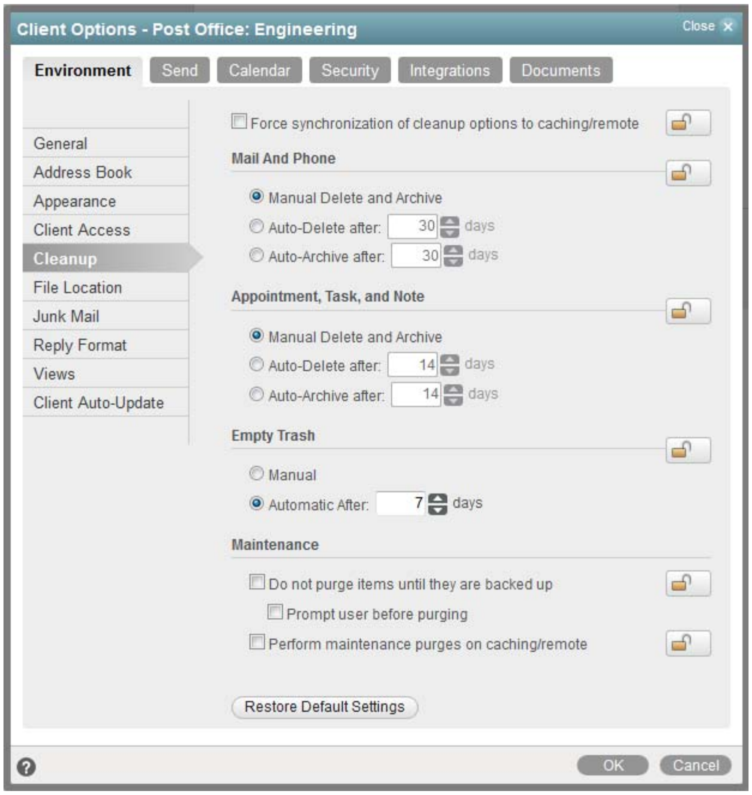
  Select the **Force Caching Mode** option (available only if the **Allow Use of Caching Mode** option is enabled) to force users to run in Caching mode. By default, this option is disabled. Specify the number of days before Caching mode is enforced. This allows the user to continue using Online mode until the grace period has passed. The grace period begins the first time the user connects to the POA. The setting applies per user per workstation.

The **Force Caching Mode** setting is not enforced on a workstation that does not have enough disk space for a Caching mailbox. The amount of disk space that is required is: the size of the mailbox + 20 MB + 25% of the mailbox size.

The **Force Caching Mode** setting is also not enforced when a user connects from a shared Windows workstation or terminal server if you configure these workstations to be excluded. You do this by setting a registry key on the Windows workstation. The registry key is in HKEY_LOCAL_MACHINE. Under `Software\\Micro Focus\\GroupWise\\Client`, add a dword value named No Local Store with a value of 1. This prevents the user from creating a Caching or Remote mailbox by using the GroupWise client menus. However, the user can still create a Caching or Remote mailbox by using the startup options /pc, /pr, or /ps.

Environment Options: Cleanup

The **Cleanup** options determine the delete and archive settings for GroupWise items (mail messages, phone messages, appointments, tasks, and notes).



Force Synchronization of Cleanup Options to Caching/Remote

Transfers the cleanup options you set in the GroupWise Admin console to users' Caching and Remote mailboxes and locks them, so that the cleanup options are performed even if users are working in their Caching or Remote mailboxes without being connected to the network.

Allow User to Protect Items from Auto Cleanup

Allows your users to set folders and items as protected. Protected folders and items are not affected by auto cleanup and auto archiving. When a folder is protected, all of the items in that folder or moved into that folder are protected. Any items moved out of the folder are no longer protected.

Mail and Phone

Choose from the following settings to determine how mail and phone messages are deleted and archived:

- **Manual Delete and Archive:** Select this option to have mail and phone messages deleted or archived only when users manually do it. This is the default setting.
- **Auto-Delete After:** Select this option to have GroupWise automatically delete mail and phone messages that are older than the specified number of days. If you use this option, you should notify users so they know they must archive items they want to save.
- **Auto-Archive After:** Select this option to have GroupWise archive mail and phone messages that are older than the specified number of days. Users must have an archive directory specified in order for items to be archived. See "Environment Options: File Location" on page 557 for information about setting a default archive directory location.

Appointment, Task, and Note

Choose from the following settings to determine how appointments, tasks, and notes are deleted or archived:

- **Manual Delete and Archive:** Select this option to have appointments, tasks, and notes deleted or archived only when users manually do it. This is the default setting.
- **Auto-Delete After:** Select this option to have GroupWise automatically delete appointments, tasks, or notes that are older than the specified number of days. If you use this option, you should notify users so they know they must archive items they want to save.
- **Auto-Archive After:** Select this option to have GroupWise automatically archive appointments, tasks, and notes older than the specified number of days. Users must have an archive directory specified in order for items to be archived. See "Environment Options: File Location" on page 557 for information about setting a default archive directory location.

Empty Trash

Deleted items are moved to the Trash folder. They can be retrieved from the Trash until it is emptied. Items in the Trash still take up disk space. Select from the following settings to determine how the Trash folder is emptied:

- **Manual:** Select this option to require the user to manually empty the Trash. This is the default setting.
- **Automatic:** Select this option to have GroupWise automatically empty items from the trash after they have been in it for the specified number of days.

Maintenance

- **Do Not Purge Items Until They Are Backed Up:** Select this option to prevent items that have not been backed up from being removed from the Trash. This option is disabled by default.

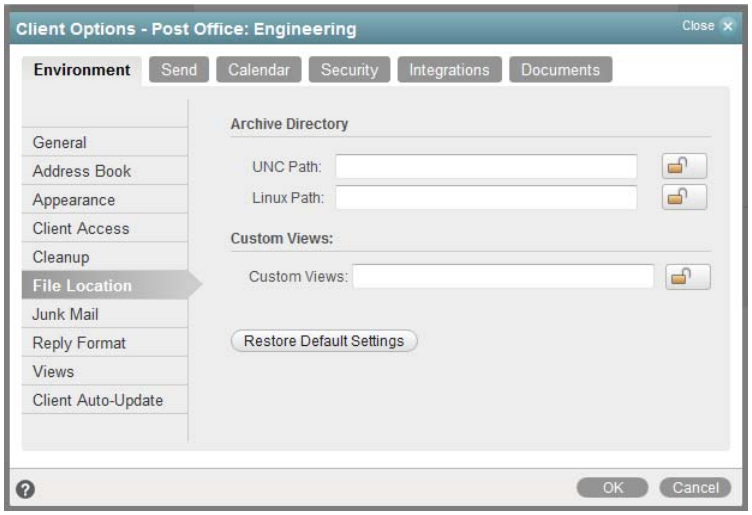
  Select the **Prompt Before Purging** option (available only if **Do Not Purge Items Until They Are Backed Up** is disabled) to prompt the user to confirm the purging of any files that have not been backed up.

* **Perform Maintenance Purges on Caching/Remote:** On the **Disk Space Management** tab (**Tools > GroupWise Utilities > Client Options > Send > Disk Space Management**) in the GroupWise Admin console, you can limit the size of users' Online mailboxes. You can now enforce the same mailbox size limits on users' Caching and Remote mailboxes, wherever those mailboxes are located.

  The size limit is applied to users' Caching and Remote mailboxes regardless of the amount of available disk space on users' hard drives. The size limit is applied the next time the GroupWise client synchronizes with users' Online mailboxes. Because users might lose items that they have been storing locally when the size limit is enforced, you should warn users that size limits are going to be placed on their local Caching and Remote mailboxes.

Environment Options: File Location

The **File Location** options determine the locations of users' archive directories and the custom views directory.



Archive Directory

Select the directory to be used for archiving items for the GroupWise client. Each user must have his or her own archive directory. You could choose a location similar to the default location for users' Caching mailbox, for example:

Windows 8:	`c:\Users\`*`user_name`*`\AppData\Roaming\Micro Focus\GroupWise\archive`
Windows 7:	`c:\Users\`*`user_name`*`\AppData\Roaming\Micro Focus\GroupWise\archive`
Windows XP:	`c:\Documents and Settings\`*`user_name`*`\Local Settings\Application Data\ Micro Focus\GroupWise\archive`

It could also be a personal user directory on a network server. If you select a network drive, ensure that users have the necessary rights to access the location.

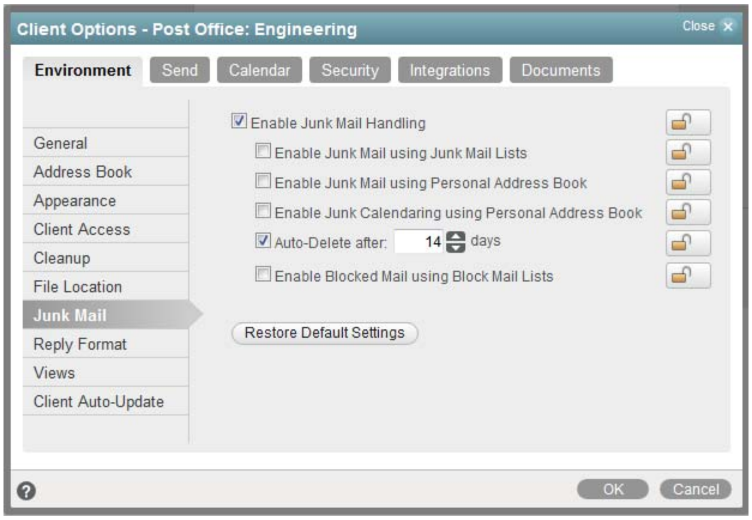
IMPORTANT: If you want to use a network location, do not specify the same directory for users in more than one post office. The names of users' individual archive directories are based on their FIDs. FIDs are unique within a post office, but users in different post offices can have the same FID.

Custom Views

This option applies only if you are using custom views. Select the directory where the views are located. The GroupWise product does not include the capability to design custom views, but third-party products make use of this feature to support their specialized capabilities.

Environment Options: Junk Mail

The Junk Mail Handling Environment options determine the junk mail handling functionality of the GroupWise client.



Junk Mail Handling

Select **Enable Junk Mail Handling** to enable junk mail handling. This setting determines whether or not the Junk Mail Handling feature is available for a user. This setting affects both the client and the POA. Junk Mail Handling allows users to block or “junk” unwanted Internet email.

When this setting is disabled, the client does not display any Junk Mail Handling menus or dialog boxes, and the POA does not perform any junk mail handling for the user. When this setting is enabled, the client displays Junk Mail Handling menus and dialog boxes, and the POA performs junk mail handling if the block and junk lists are also enabled.

Enable Junk Mail Using Junk Mail Lists

Select this option to cause junking based on email addresses and domain names available to users. A user can junk email from a specific Internet email address or from an entire Internet domain, when the email addresses and Internet domains are listed in the user’s Junk List. (Initially, there are no entries in a user’s junk list.) Junked items are delivered to the Junk Mail folder in the user’s Mailbox.

When this setting is enabled or disabled and not locked, the user’s initial setting to use the Junk List is enabled or disabled. Users can change the setting. When the setting is enabled and locked, a user's Enable Junk List setting is enabled and cannot be disabled. When the setting is disabled and locked, the Junk List is unavailable to the user. Client menu options and dialog boxes involving the Junk List are not displayed.

Enable Junk Mail Using Personal Address Book

Select this option to cause junking based on personal address book entries available to users. A user can junk email from all users whose addresses are not in any personal address books (including Frequent Contacts) without building a Junk List.

When this setting is enabled or disabled and not locked, the user's initial setting to use personal address books is enabled or disabled. Users can change the setting. When the setting is enabled and locked, a user's **Enable Junk Mail Using Personal Address Book** setting is enabled and cannot be disabled. When the setting is disabled and locked, this option is unavailable to the user.

Enable Junk Calendaring Using Personal Address Book

Select this option to make junking of calendar items based on personal address book entries available to users. A user can junk calendar items from all users whose addresses are not in any personal address books (including Frequent Contacts) without building a Junk List.

Auto-Delete After

Select this option and specify the number of days after which you want junked items to be automatically deleted from users' mailboxes. The default is 14 days.

When this setting is enabled or disabled and not locked, the user's initial setting to delete junked items is enabled or disabled. Users can change the setting. When the setting is enabled and locked, a user's **Automatically Delete Items** setting is enabled and cannot be disabled. When the setting is disabled and locked, this option is unavailable to the user.

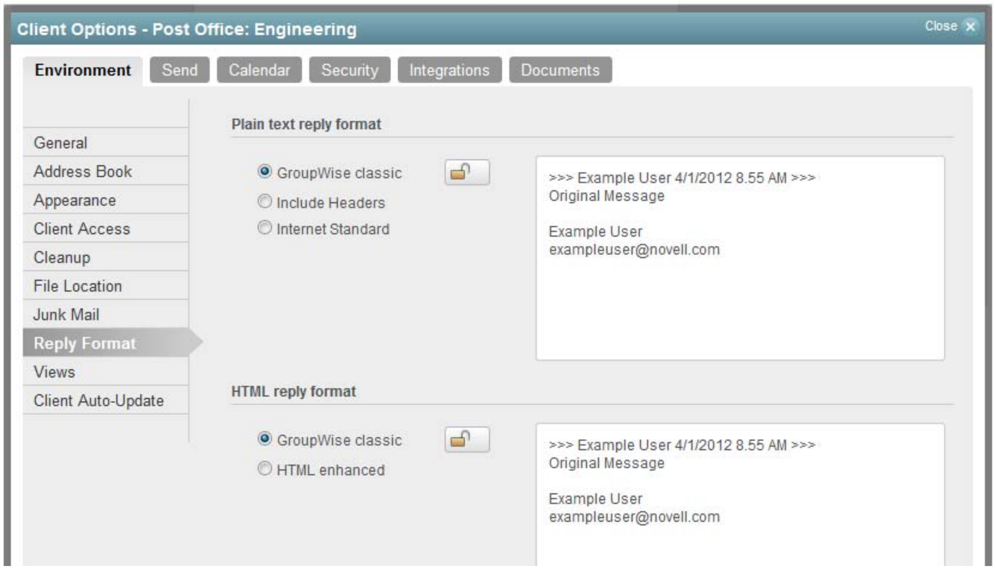
Enable Blocked Mail Using Block Mail Lists

Select this option to make blocking available to users. A user can block email from an Internet email address or Internet domain, when blocked email addresses and Internet domains are listed in the user's Block List. (Initially, there are no entries in a user's Block List.) Blocked items are blocked when the POA processes delivery to the user's mailbox, and the items are never delivered to the user's mailbox. When the POA log uses verbose mode, the log displays information about blocked items.

When this setting is enabled or disabled and not locked, the user's initial setting to use the Block List is enabled or disabled. Users can change the setting. When the setting is enabled and locked, a user's Block List setting is enabled and cannot be disabled. When the setting is disabled and locked, blocking is unavailable to the user. Client menu options and dialog boxes involving the Block List are not displayed.

Environment Options: Reply Format

In the GroupWise client, users can set the format that they want to use for replies to GroupWise items. For more information, see "Setting the Default Reply Format" in the *GroupWise 18 Client User Guide*. The Reply Format options in the GroupWise Admin console control which reply format options are available to users in the GroupWise client.



Plain Text Reply Format

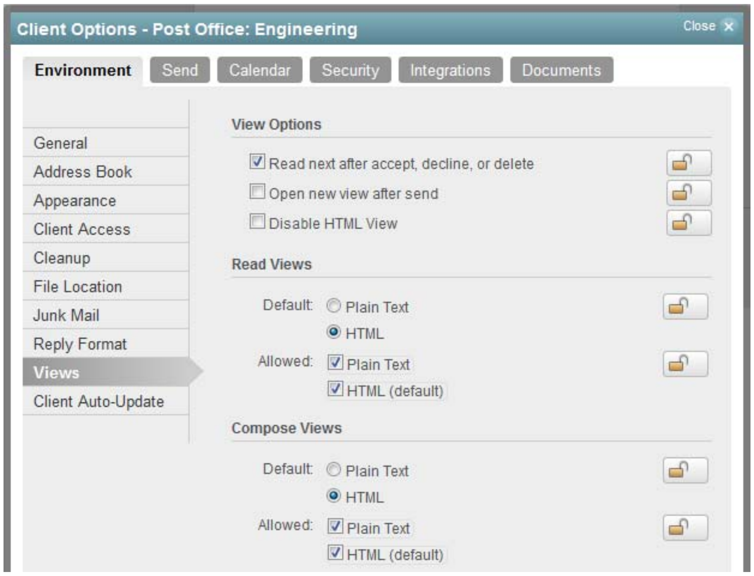
- **GroupWise Classic:** Provides separator characters, original sender, date, and time.
- **Include Headers:** Allows the selection of the separator character; provides the original sender, recipient, date, time, and subject.
- **Internet Standard:** Allows the selection of the separator character; allows you to include the original sender, email address, date, time, and message identifier.

HTML Reply Format

- **GroupWise Classic:** Provides separator characters, original sender, date, and time.
- **HTML Enhanced:** Allows the selection of the separator character; allows you to include the original sender, email address, date, time, and message identifier. Select **Include Headers** to provide the original sender, recipient, date, time, and subject instead.

Environment Options: Views

The **Views** Environment options determine when items open, and whether or not users can read and compose messages in HTML.



View Options

Choose from the following settings to determine what occurs when the user performs an action that closes the current view.

- **Read Next after Accept, Decline, or Delete:** Select this option to have the next available received item automatically open after the user accepts, declines, or deletes an appointment, task, or note. By default, this option is enabled.
- **Open New View after Send:** Select this option to have a new send view open after a user sends a message. By default, this option is disabled.
- **Disable HTML View:** Select this option to turn off the ability to view or compose messages in HTML View.

Allowable Read Views

Choose from the following settings to determine what read views you allow the clients to use.

- **Plain Text (Default):** Select this option to allow users to read items in plain text.
- **HTML:** Select this option to allow users to read items in HTML.

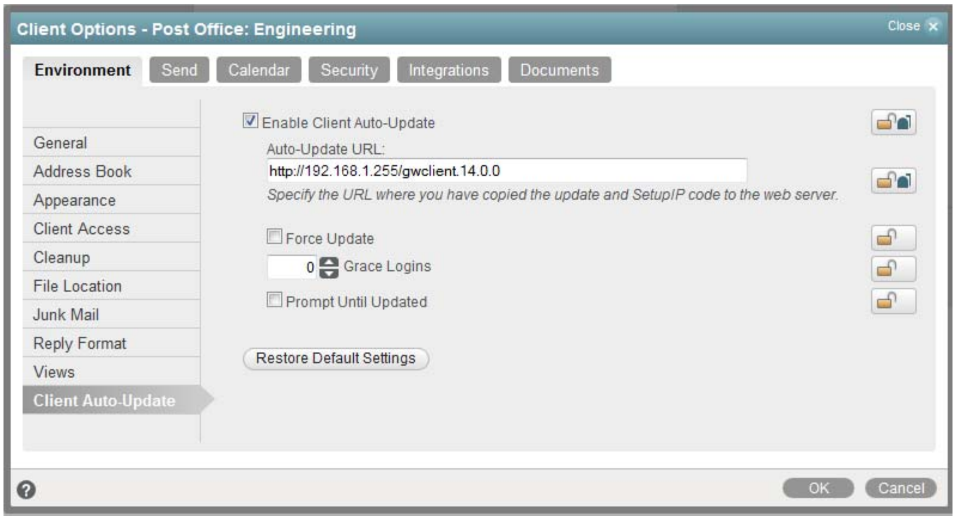
Allowable Compose Views

Choose from the following settings to determine what compose views you allow the clients to use.

- **Plain Text (Default):** Select this option to allow users to compose items in plain text.
- **HTML:** Select this option to allow users to compose items in HTML.

Environment Options: Client Auto-Update

The GroupWise client includes the Client Auto-Update feature that helps you keep users' GroupWise client software up to date. Each time the GroupWise client starts, it checks with the POA for the user's post office to find out if new GroupWise client software is available. When new software is available and Client Auto-Update is enabled, the GroupWise client can prompt the user to install the updated software.



For complete usage instructions, see "Using Client Auto-Update to Distribute the GroupWise Client Software" on page 583.

Enable Client Auto-Update

Configures GroupWise so that GroupWise client software updates are automatically handled according to the Client Auto-Update settings.

The GroupWise client software can be installed along with the POA software for each post office, and the Client Auto-Update functionality is triggered at the post office level. If necessary, you can enable and configure it at the domain level so that it functions consistently across all post offices in each domain.

Auto-Update URL

(Optional) Specify the URL where the GroupWise client software can be distributed by your web server. You can use the same URL for multiple domains and post offices, or you can specify different URLs for different domains and post offices.

If Client Auto-Update is enabled but no URL is specified, the POA distributes the GroupWise client software to users' workstations. This can be convenient in a small GroupWise system, because no web server setup is required. However, it places an additional load on the POA whenever client software updates are called for.

Force Update

Automatically updates users' GroupWise client software without prompting users.

Users can still click Cancel to cancel the update. However, they cannot run the GroupWise client to access their mailboxes until they update the software

Grace Logins

(Conditional) If Force Update is selected, specify the number of grace logins allowed before you require the users to update their GroupWise client software

Prompt Until Updated

Causes the GroupWise client to prompt the user to update the GroupWise client software each time the client starts. The user can choose not to install the new software when prompted and still run the currently installed version of the client. However, the Client Auto-Update reminder appears the next time the user starts the client.

You can customize the Client Auto-Update settings at the user level to tailor the Client Auto-Update experience for individual users. For example, you might not want to force the software update for selected users, or perhaps you want to allow more grace logins for selected users.

Modifying Send Options

1. In the GroupWise Admin console, display the Client Options **Send** tab.

   For instructions, see Chapter 69, “Setting Defaults for the GroupWise Client Options,” on page 545.

2. Click the tab that contains the options that you want to change:

   “Send Options: Send Options” on page 564
   “Send Options: Mail” on page 566
   “Send Options: Appointment” on page 567
   “Send Options: Task” on page 568
   “Send Options: Note” on page 569
   “Send Options: Disk Space Management” on page 570
   “Send Options: Global Signature” on page 571
   “Send Options: Security” on page 572

3. If you want to prevent users from changing an option’s setting, click the lock button next to it.

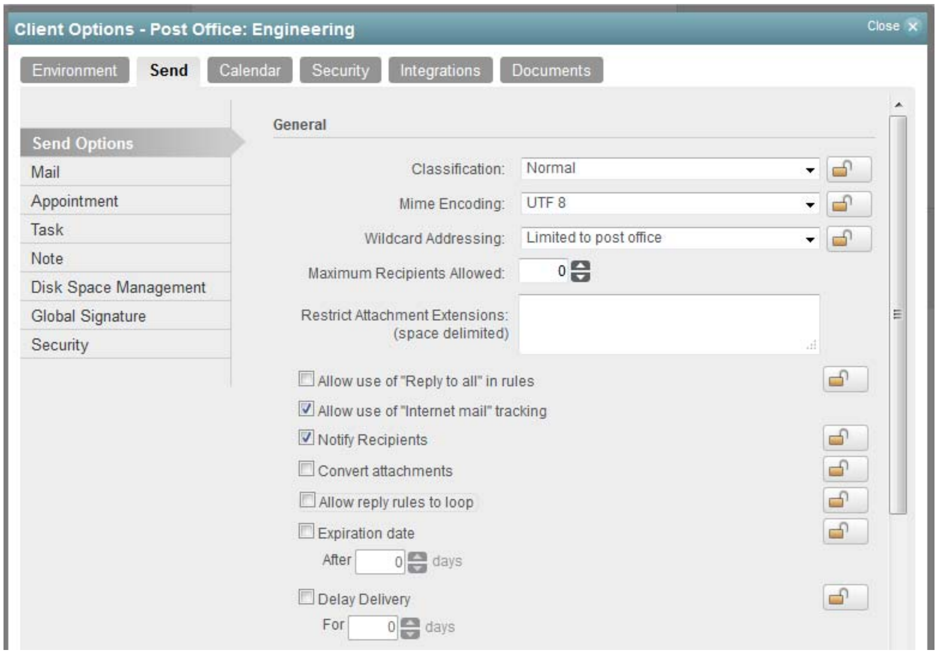
   After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.

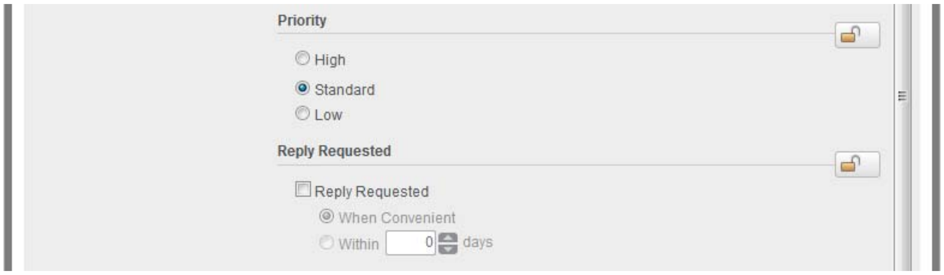
4. If you want to return all the options on a tab to their default settings, click **Restore Default Settings**.

5. When you are finished, click **OK** to save your changes.

Send Options: Send Options

The **Send Options** determine general settings that apply to all GroupWise item types (mail messages, phone messages, appointments, tasks, and notes).





Classification

Select the default for the security classification label at the top of the message box. The classifications do not provide any encryption or additional security. They are meant to alert the recipient to the relative sensitivity of the item. The options are **Normal**, **Proprietary**, **Confidential**, **Secret**, **Top Secret,** and **For Your Eyes Only.** The default is **Normal**.

MIME Encoding

Select the default MIME encoding for all outgoing messages. The MIME encoding is used to specify the character set that is used for all outgoing messages. This is important when your company has users who are using different character sets. For more information, see "MIME Encoding" on page 88.

Wildcard Addressing

Wildcard addressing enables a user to send an item to all users in a post office, domain, GroupWise system, or connected GroupWise system by inserting asterisks (*) as wildcards in email addresses.

- **Not Allowed:** Select this option to disable wildcard addressing.
- **Limited to Post Office (Default):** Select this option to limit wildcard addressing to the user's post office. This means that a user can send an item to all users on the same post office by entering * in the item's address field.
- **Limited to Domain:** Select this option to limit wildcard addressing to the user's domain. This means that a user can send an item to all users in the domain by entering *.* in the item's address field. A user can also send an item to all users on another post office in the domain by entering *.*post_office_name* in the item's address field.
- **Limited to System:** Select this option to limit wildcard addressing to the user's GroupWise system. This means that a user can send an item to all users in the GroupWise system by entering *.*.* in the item's address field. A user can also send an item to all users in another domain by entering *.*domain_name* or to all users in another post office by entering *.*post_office_name*.
- **Unlimited:** Select this option to allow unlimited use of wildcard addressing. This means that a user can send an item to all users in another GroupWise system by entering *.*post_office_name.domain_name* or *.*domain_name* in the item's address field.

Maximum Recipients Allowed

By default, users can send messages to any number of recipients. To prevent users from sending messages to very large numbers of users, perhaps using groups or wildcard addressing, specify the maximum number of recipients that a message can be sent to. If users exceed the specified maximum, they receive an error instructing them to remove recipients and try again.

Restrict Attachment Extensions

To prevent users from sending specific types of attachments, such as executables, media files, and so on, specify the file extensions that cannot be attached to messages. If users attach a restricted file type, they receive an error indicating the file type restriction, so that they can remove the attachment.

Allow Use of "Reply to All" in Rules

Select this option to enable users to use the **Reply to All** action when creating rules. By default, this option is disabled, which means that only the **Reply to Sender** action is available.

Allow Use of "Internet Mail" Tracking

Select this option to allow users' GroupWise clients to automatically embed information in Internet-bound items. The embedded information instructs the receiving system to send back a delivery notification message (if it is supported). By default, this option is enabled.

For this option to work, the Enable Delivery Confirmation option must be enabled in the GroupWise client (**Tools > Options > Send Options > Mail > Enable Delivery Confirmation**). This is the default setting.

Notify Recipients

Select this option to have recipients notified when they receive an item, if they are using GroupWise Notify. By default, this option is enabled.

Convert Attachments

Select this option to allow conversion of attachments in items sent to non-GroupWise email systems through a GroupWise gateway.

Allow Reply Rules to Loop

By default, GroupWise does not allow a rule-generated reply to be replied to by another rule-generated reply. This situation, referred to as looping, can quickly increase message traffic. To allow reply rules to loop, select this option.

Expiration Date

Select this option to have unopened messages expire after the specified number of days. By default, this option is disabled.

Delay Delivery

Select this option to delay the delivery of messages for the specified number of days. For example, if you specify 3 days, a message is not delivered until 3 days after the day it is sent. Messages are delivered at 12:01 a.m. of the appropriate day. By default, this option is disabled.

Priority

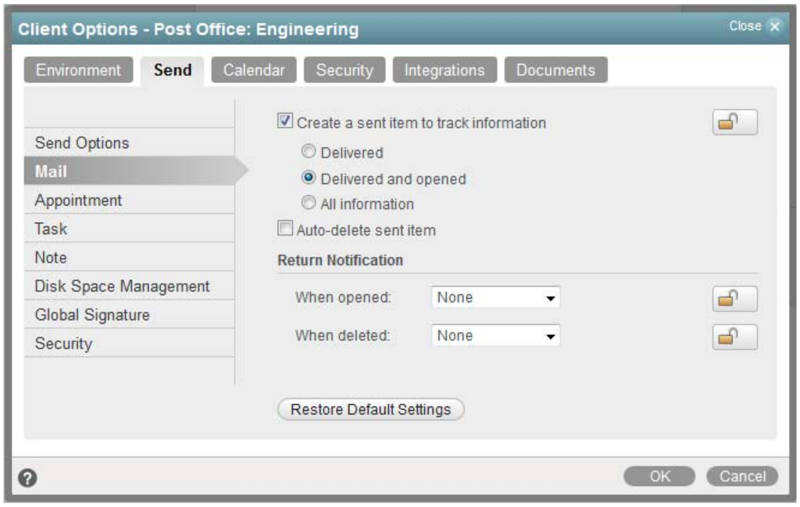
Select **High**, **Standard**, or **Low** as the default item priority. Priority determines which post office directory an item is placed in. This, in turn, determines how quickly items are delivered. High priority items are queued ahead of normal or low priority items.

Reply Requested

Select the **Reply Requested** option to have items always include a reply request. By default, this option is disabled. If you enable the option, select whether the recipient is asked to reply when it is convenient or within a specific number of days.

Send Options: Mail

The **Mail** options apply to mail and phone messages only.



Create a Sent Item to Track Information

By default, items the user sends are inserted in the user's Sent Items folder. Deselect this option if you do not want the items placed there. If items are not placed in the Sent Items folder, users cannot check the delivery status of the item. The following options are available only if this option is selected.

- **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the message to view the status.
- **Delivered and Opened (Default):** Select this option to track delivered and opened status only. The user can open the Properties window of the sent message to view the status.
- **All Information:** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the message to view the status.
- **Auto-Delete Sent Item:** Select this option to automatically delete messages from the user's Mailbox after all the recipients have deleted the messages and emptied them from the Trash.

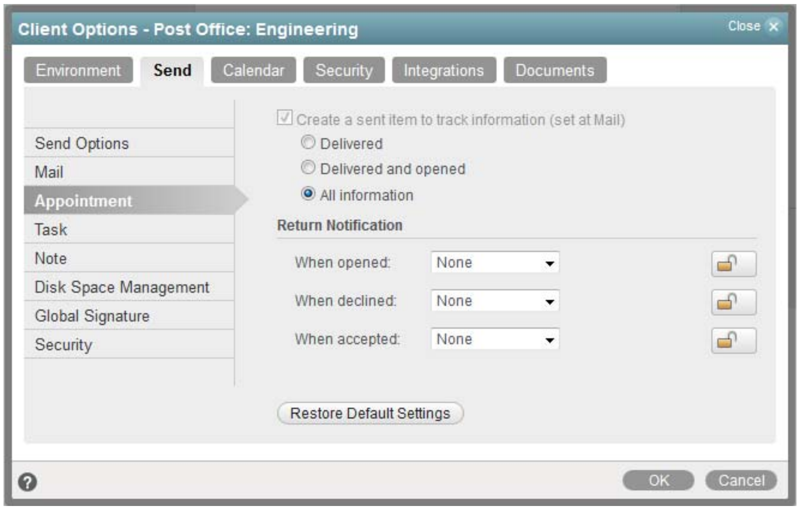
Return Notification

In addition to status tracking information, the user can receive notification when a message is opened or deleted. Choose from the following notification options:

- **None (Default):** The user does not receive notification.
- **Mail Receipt:** The user receives a mail message stating that the recipient opened or deleted the message.
- **Notify:** The user receives notification through GroupWise Notify when the recipient opens or deletes the message.
- **Notify and Mail:** The user will receive notification through GroupWise Notify and a mail message.

Send Options: Appointment

The **Appointment** options apply to appointments only.



Create a Sent Item to Track Information

The setting for this option is inherited from the setting on the **Mail** tab; it can only be enabled or disabled on the **Mail** tab. If the option is enabled, you can choose from the following status tracking levels:

- **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the appointment to view the status.
- **Delivered and Opened:** Select this option to track delivered and opened status only. The user can open the Properties window of the appointment to view the status.
- **All Information (Default):** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the appointment to view the status.

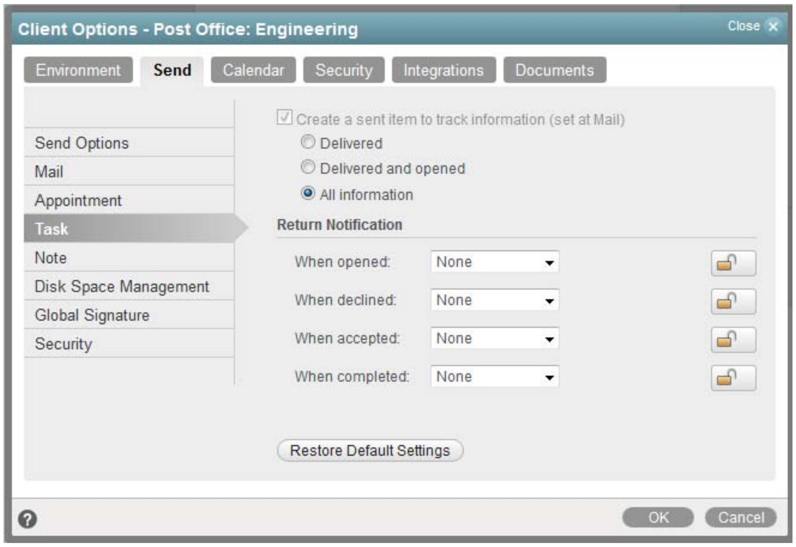
Return Notification

In addition to status tracking information, the user can receive notification when an appointment is opened, accepted, or deleted. Choose from the following notification options:

- **None (Default):** The user does not receive notification.
- **Mail Receipt:** The user receives a mail message stating that the recipient opened, accepted, or deleted the appointment.
- **Notify:** The user receives notification through GroupWise Notify when the recipient opens, accepts, or deletes the appointment.
- **Notify and Mail:** The user receives notification through GroupWise Notify and a mail message.

Send Options: Task

The **Task** options apply to tasks only.



Create a Sent Item to Track Information

The setting for this option is inherited from the setting on the **Mail** tab; it can only be enabled or disabled on the **Mail** tab. If the option is enabled, you can choose from the following status tracking levels:

- **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the task to view the status.
- **Delivered and Opened:** Select this option to track delivered and opened status only. The user can open the Properties window of the task to view the status.
- **All Information (Default):** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the task to view the status.

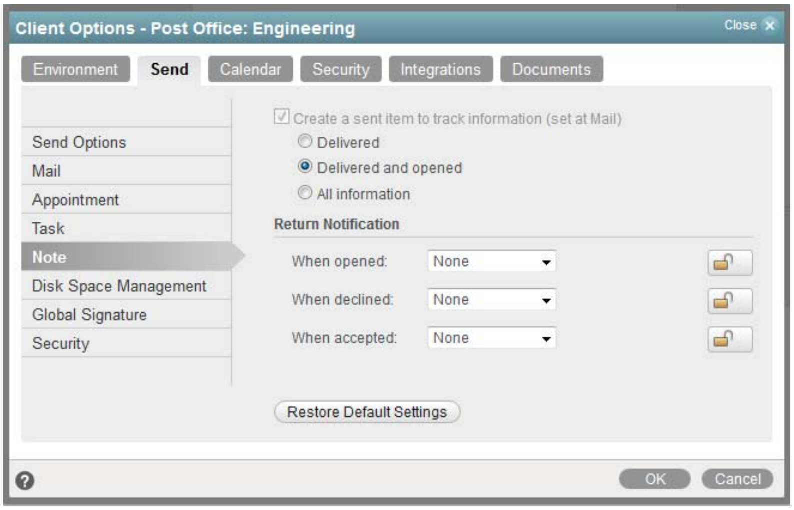
Return Notification

In addition to status tracking information, the user can receive notification when a task is opened, accepted, completed, or deleted. Choose from the following notification options:

- **None (Default):** The user does not receive notification.
- **Mail Receipt:** The user receives a mail message stating that the recipient opened, accepted, completed, or deleted the task.
- **Notify:** The user receives notification through GroupWise Notify when the recipient opens, accepts, completes, or deletes the task.
- **Notify and Mail:** The user receives notification through GroupWise Notify and a mail message.

Send Options: Note

The **Note** options apply to notes only.



Create a Sent Item to Track Information

The setting for this option is inherited from the setting on the **Mail** tab; it can only be enabled or disabled on the **Mail** tab. If the option is enabled, you can choose from the following status tracking levels:

- **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the note to view the status.

* **Delivered and Opened (Default):** Select this option to track delivered and opened status only. The user can open the Properties window of the note to view the status.
* **All Information:** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the note to view the status.

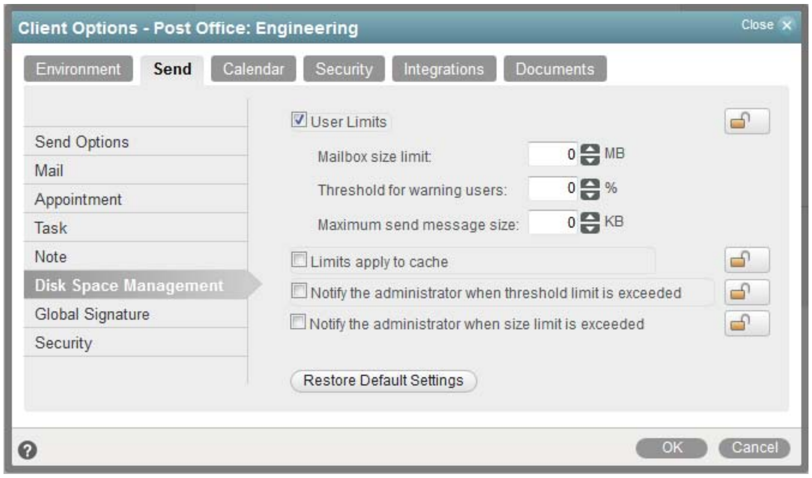
Return Notification

In addition to status tracking information, the user can receive notification when a note is opened or deleted. Choose from the following notification options:

* **None (Default):** The user does not receive notification.
* **Mail Receipt:** The user receives a mail message stating that the recipient opened or deleted the note.
* **Notify:** The user receives notification through GroupWise Notify when the recipient opens or deletes the note.
* **Notify and Mail:** The user receives notification through GroupWise Notify and a mail message.

Send Options: Disk Space Management

The **Disk Space Management** options let you enforce disk space limitations for users on a post office.



User Limits

Select this option if you want to impose limits on the size of users' mailboxes or the size of messages they can send. By default, this option is disabled, so there are no size limits. If you enable it, you can modify the following options:

* **Mailbox Size Limit:** Specify the maximum amount of post office disk space available to each user for storing message and attachment files. The setting uses logical disk space because attachments are shared by all recipient users on the same post office. Messages in shared folders are counted as disk space only for the owner of the shared folder. If you do not want to limit the mailbox size, set the value to zero (0). The physical maximum size limit for a mailbox is 4 TB.

  If users meet or exceed their mailbox size limits, they cannot send items until their mailboxes are under the size limit. Users can reduce the size of their mailboxes by deleting or archiving items.

- **Threshold for Warning Users:** Select the mailbox capacity (as a percentage) that must be reached before the user is warned that his or her mailbox is reaching its limit. For example, if the mailbox size limit is 200 MB and the threshold is set at 75%, users receive warnings when their mailboxes reach 150 MB. Set the value to 0 or 100 if you do not want users to receive a warning.
- **Maximum Send Message Size:** Specify the maximum size of a message (in kilobytes) that a user can send using the GroupWise client. If the user sends an item that exceeds this size, a message notifies the user that the item is too large to send.

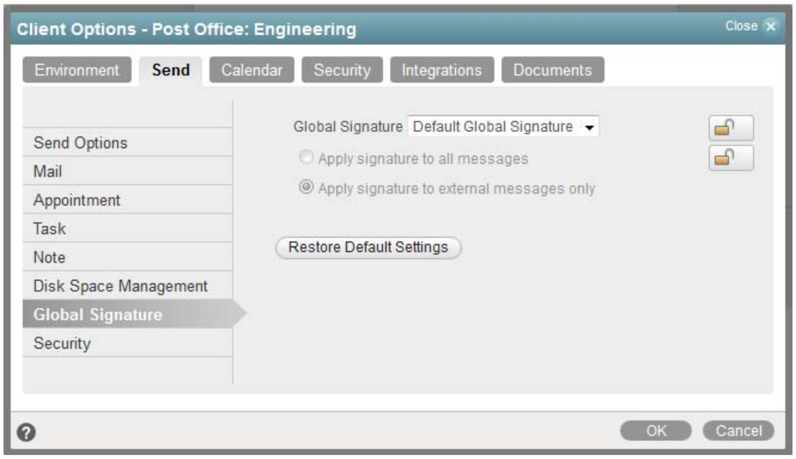
  You can also set message size limits at the post office level through POA configuration, at the domain level through MTA configuration, and at the GroupWise system level through GWIA configuration. For more information, see "Restricting the Size of Messages That Users Can Send" on page 125.
- **Limits Apply to Cache:** Select this option to prevent users from sending from their Caching or Remote mailboxes when their Caching or Remote mailboxes exceed the limits you have set for Online mailboxes. For more information, see "Enforcing Mailbox Size Limits" on page 124. You can use this option in conjunction with the **Perform Maintenance Purges on Caching/Remote** option to control the size of users' Caching and Remote mailboxes.

  If you impose this limit on users who have existing Caching or Remote mailboxes, their Caching or Remote mailboxes might be reduced in size in order to meet the new disk space limit. Such users should be warned in advance so that they can back up their Caching or Remote mailboxes before the size reduction takes place. Otherwise, users could lose messages that they want to keep.
- **Notify the Administrator When Threshold Limit Is Exceeded:** Select this option so that the domain's notification user is notified along with the mailbox owner when the user's mailbox exceeds the size established in the **Threshold for Warning Users** field. The domain's notification user who receives the notification must be defined on the **General** tab of the Domain object.
- **Notify the Administrator When Size Limit Is Exceeded:** Select this option so that the domain's notification user is notified when the user's mailbox exceeds the size established in the **Mailbox Size Limit** field. The domain's notification user who receives the notification must be defined on the **General** tab of the Domain object.

  For more information about notification users, see "Receiving Notifications of Agent Problems" on page 242.

Send Options: Global Signature

The **Global Signature** option lets you set the global signature. To set options at the domain level, select a domain. To set options at the post office level, select a post office. To set options for individual users, select one or more users.



Global Signature

1. Select a global signature to append to users' messages.

   When enabled, global signatures are automatically appended to every message that is sent by the users. For more information, see "Global Signatures" on page 52.

2. Select **Apply the signature to all messages** to add the signature to all internal or external messages.

   or

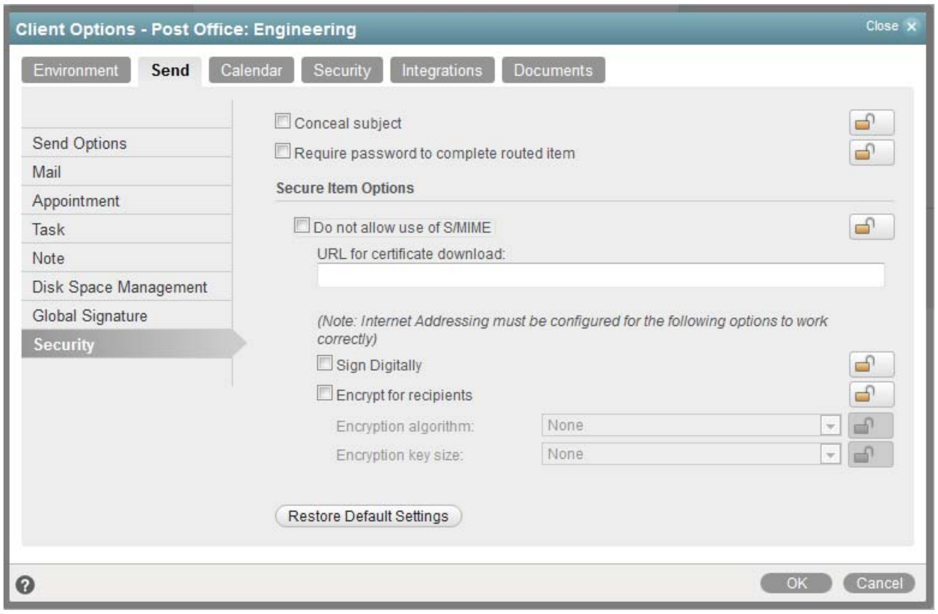
   Select **Apply signature to external messages only** to apply the signature to messages that are sent through the GWIA.

If you select **Default Global Signature,** the default signature that is used by the GWIA is applied. If you select **None**, then no signature is applied.

NOTE: All **Global Signature** options pertain only to the GroupWise client.

Send Options: Security

The **Security** options apply to all GroupWise item types (mail messages, phone messages, appointments, tasks, and notes).



Conceal Subject

Select this option to conceal the item's subject so the notification that appears on the recipient's screen does not include the subject. The subject of the item is also concealed in the recipient's mailbox and the sender's Sent Items folder. It is visible only when the item is being read.

Require Password to Complete Routed Item

Select this option to require a user to enter a password before completing a routed item.

Secure Items Options

If users have installed security providers on their workstations, select the options you want them to use.

- **Do Not Allow Use of S/MIME:** Select this option to disable S/MIME functionality. This disables the **Encrypt** and **Digitally Sign** buttons (and other related S/MIME functionality) in the GroupWise client. By default, this option is enabled. When it is enabled, you can modify the rest of the options in the dialog box.
- **URL for Certificate Download:** Specify the Internet address of your preferred certification authority. If it is not otherwise changed in this field, the GroupWise client accesses http://www.novell.com/groupwise/certified.html, which lists several common certification authorities.
- **Sign Digitally:** Select this option to enable users to add a digital signature to their outgoing messages. Recipients of a digitally signed item who have S/MIME-enabled email products are able to verify that the item is actually from the sender. This setting is not a useful security measure unless you lock it as the default.
- **Encrypt for Recipients:** Select this option to enable users to encrypt an outgoing item so they can ensure that the intended recipients who have an S/MIME-enabled email product are the only individuals who can read the item. This setting is not a useful security measure unless you lock it as the default.

  If you enable the **Encrypt for Recipients** options, you can set the encryption algorithm and key size. The available algorithm methods (RC2, RC4, DES, 3DES) are trusted algorithms that encrypt or transform data to mask the original content. The key size sets the default size (in bits) of the encryption key that is used with the algorithm you select. These settings are not useful security measures unless you lock them.

Modifying Calendar Options

1 In the GroupWise Admin console, display the Client Options **Calendar** tab.

   For instructions, see Chapter 69, “Setting Defaults for the GroupWise Client Options,” on page 545.

2 Click the tab that contains the options that you want to change:

   “Calendar Options: General” on page 574
   “Calendar Options: Web Calendar” on page 575
   “Calendar Options: Busy Search” on page 576

3 If you want to prevent users from changing an option’s setting, click the lock button next to it.

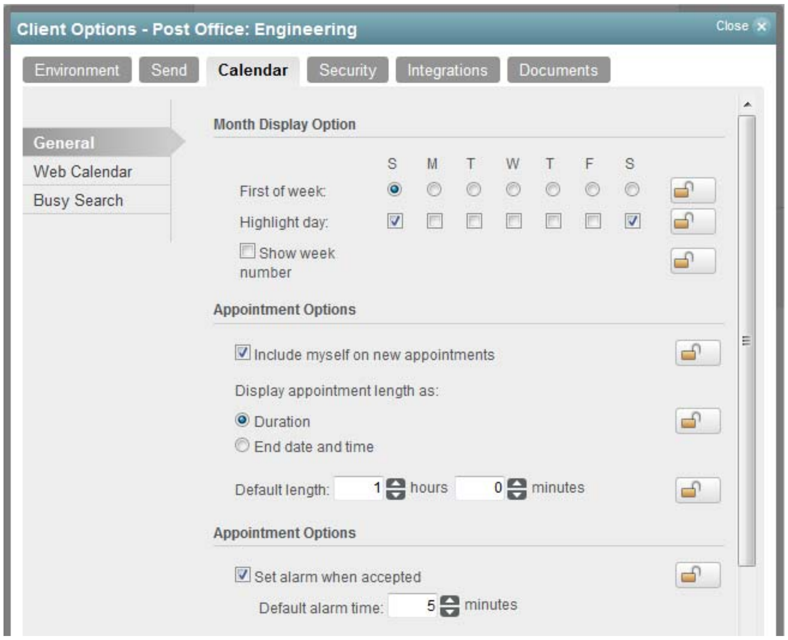
   After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.

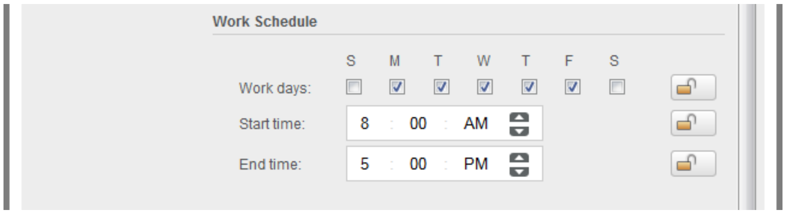
4 If you want to return all the options on a tab to their default settings, click **Restore Default Settings**.

5 When you are finished, click **OK** to save your changes.

Calendar Options: General

The General options determine basic settings for the GroupWise Calendar.





Month Display Option

Select from the following options to determine how the month calendar is displayed:

- **First of Week:** Select the day of the week that you want to display as the first day on the calendar.
- **Highlight Day:** Select any days you want highlighted, such as weekends and holidays.
- **Show Week Number:** Select this option to display the week number (1 through 52) at the beginning of the calendar week.

Appointment Options

Select from the following options to determine how appointments are handled:

- **Include Myself on New Appointments:** Select this option to have the sender automatically included in the appointment’s To: list. This option is enabled by default.
- **Display Appointment Length As:** When creating an appointment, the sender must specify the appointment’s length. You can use this option to determine whether the sender enters a duration for the appointment or an end time for the appointment. Select the Duration setting to have appointments display a Duration field that the sender must fill in (for example, 30 minutes, 1

hour, or 10 hours). Select the **End Date and Time** setting to have appointments display **End Date and Time** fields that the sender must fill in (for example, June 3, 18 and 10:00 a.m.). The default setting is **Duration**.

- **Default Length:** Select the default length for appointments. Users can change the length. If the appointment's length is displayed as a duration, the duration defaults to this length. If it is displayed as an end date and time, the end time defaults to the start time plus the default length (for example, if the start time is 9:00 a.m. and the default length is 1 hour, the end time defaults to 10:00 a.m).

Alarm Options

Users can set appointment alarms so that they are notified prior to an appointment time. Select from the following options to determine the default settings for an alarms:

- **Set Alarm When Accepted:** Select this option to have an alarm automatically set when the user accepts an appointment. By default, this option is enabled.
- **Default Alarm Time:** Select the number of minutes before an appointment to notify the user. The default is 5 minutes.

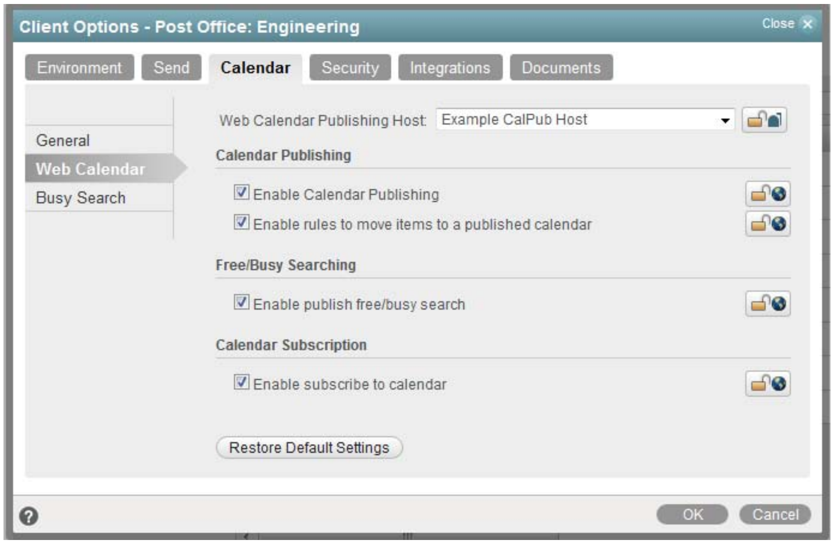
Work Schedule

The work schedule determines the user's normal work days and hours. In the calendar and during busy searches, any days or hours outside of the work schedule are represented by gray squares (Out of Office). Users can still be scheduled for appointments during non-work hours.

- **Work Days:** Select the work days. The start time and end time are applied to each work day.
- **Start Time:** Select the daily start time. The default is 8:00 a.m.
- **End Time:** Select the daily end time. The default is 5:00 p.m.

Calendar Options: Web Calendar

The Calendar options enable various types of calendar publishing for GroupWise users.



Web Calendar Publishing Host

Select the Calendar Publishing Host for this domain or post office from the drop-down list. For setup instructions, see "Setting Up the GroupWise Calendar Publishing Host" in the *GroupWise 18 Installation Guide*.

Enable Calendar Publishing

Select this option to let users publish personal GroupWise calendars on the Internet. When calendar publishing is enabled, users of the GroupWise client and GroupWise WebAccess can right-click a personal calendar, then click **Publish** to select options for publishing a personal calendar.

Enable Rules to Move Items to a Published Calendar

Select this option to allow users to create rules that move specific items to a published GroupWise calendar. Rules are disabled by default.

Enable Publish Free/Busy Search

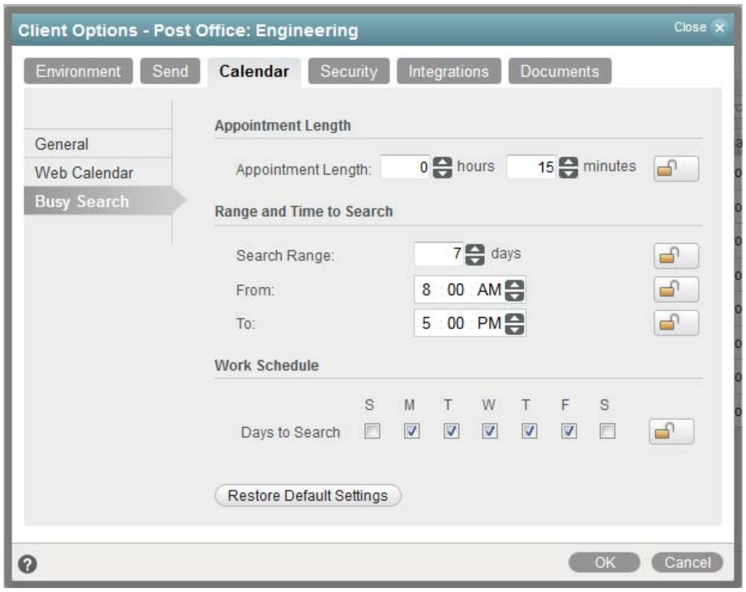
Enable this option to allow users to make their appointment information available to external users, so that external users can perform Free/Busy Searches on users' GroupWise calendars. Free/Busy searching is disabled by default.

Enable Subscribe to Calendar

Select this option to allow users to subscribe to Internet calendars that are updated on a regular basis, such as calendars for sporting events. Calendar subscription is enabled by default. Calendar subscription can be enabled even if no Calendar Publishing Host has been selected.

Calendar Options: Busy Search

The **Busy Search** options determine the amount of free time required for the appointment and the range of dates to search.



Appointment Length

Set the default appointment length to search. You can set the length in 15-minute increments. The default is 15 minutes. This setting is used only when the user does a busy search through the **Busy Search** option on the **Tools** menu. Otherwise, the default appointment length defined on the **Calendar** tab is used (see "Calendar Options: General" on page 574).

Range and Time to Search

Specify the number of days to include in the search, then set the daily start and end times for the search.

Work Schedule

Select the days to search. By default, the typical work days (Monday through Friday) are selected.

Modifying Security Options

1. In the GroupWise Admin console, display the Client Options **Security** tab.

   For instructions, see Chapter 69, "Setting Defaults for the GroupWise Client Options," on page 545.
2. Click the tab that contains the options that you want to change:

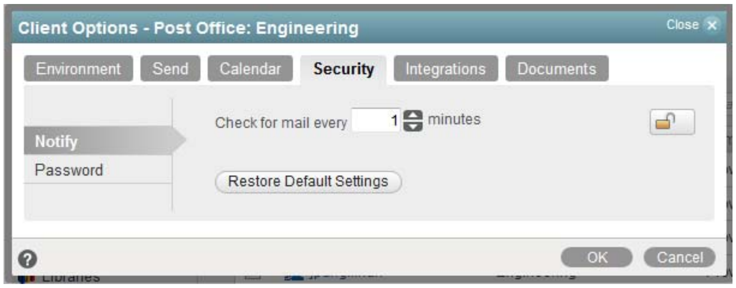
   "Security Options: Password" on page 578
   "Security Options: Notify" on page 577
3. If you want to prevent users from changing an option's setting, click the lock button next to it.

   After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.
4. If you want to prevent users from changing an option's setting, click the lock button next to it.

   After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.
5. When you are finished, click **OK** to save your changes.

Security Options: Notify

The **Notify** option determines how often GroupWise Notify checks a user's mailbox for newly received items. If new items are detected, the user is notified. The default is every minute.



Security Options: Password

The **Password** options let you reset a user's password and enable various methods by which a user can set up the GroupWise client so that he or she does not have to enter a password at startup.

For background information about passwords, see Chapter 89, "GroupWise Passwords," on page 687.

Password / Confirm Password

If a user forgets his or her GroupWise password, you can provide the user with a new password to access GroupWise. You should advise the user to change the new password to a personal one.

Clear User Password

If a user forgets his or her personal password, select this option to clear the password. The user can then enter a new password at his or her discretion. In a high security post office, it might be necessary to set a new password after clearing the old one.

Allow eDirectory Authentication Instead of Password

Select this option to allow users to select the **No Password Required with eDirectory** option under Security options in the GroupWise client. When this option is selected in the client, the user can access his or her mailbox without requiring a password if he or she is already logged in to Micro Focus eDirectory. Mailbox access is granted based on eDirectory authentication, not on password information. This option is available only if eDirectory authentication is enabled for the post office. For more information, see "Configuring Post Office Security" on page 150.

Enable Single Sign-On

Select this option to give users the **Use Single Sign-on** option under **Security Options** in the GroupWise client. This option lets the user access his or her mailbox without reentering the password. After a user selects **Use Single Sign-On** in the GroupWise client, the GroupWise password is stored in eDirectory for the currently logged-in user.

IMPORTANT: Micro Focus Single Sign-on must be installed on the user's workstation in order for this option to take effect.

Use Collaboration Single Sign-on (CASA)

Select this option to give users the **Use Collaboration Single Sign-on (CASA)** option under **Security Options** in the GroupWise client. This option lets the user access his or her mailbox without reentering the password if the **Collaboration Single Sign-on (CASA)** software is installed. After a user selects **Use Collaboration Single Sign-On (CASA)** in the GroupWise client and if the CASA client is installed, the GroupWise password is stored for the currently logged-in user.

Modifying Integrations Options

1 In the GroupWise Admin console, display the Client Options **Integrations** tab.

   For instructions, see Chapter 69, "Setting Defaults for the GroupWise Client Options," on page 545.

2 Click the tab that contains the options that you want to change:

   "Security Options: Notify" on page 577
   "Security Options: Password" on page 578

3 If you want to prevent users from changing an option's setting, click the lock button next to it.

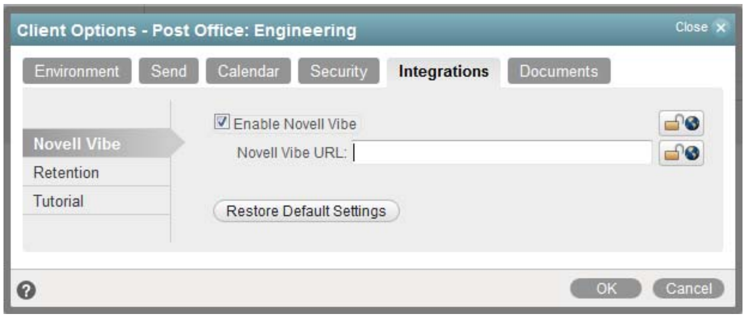
   After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.

4 If you want to return all the options on a tab to their default settings, click **Restore Default Settings**.

5 When you are finished, click **OK** to save your changes.

Integrations Options: Micro Focus Vibe

The Micro Focus Vibe options provide access to a Micro Focus Vibe site for GroupWise users. Micro Focus Vibe enhances GroupWise by providing easy document management and sharing, team calendars and task lists, workflows, discussion threads, wikis, blogs, and RSS feeds.



Enable Micro Focus Vibe

Select this option to provide GroupWise client users with a Micro Focus Vibe folder in their mailboxes. The Micro Focus Vibe folder links to the Micro Focus Vibe site associated with your GroupWise system. For more information, see "Enabling GroupWise/Vibe Integration for GroupWise Client Users" in the *GroupWise 18 Interoperability Guide*.

Micro Focus Vibe URL

Specify the URL of the Micro Focus Vibe site. The following format is required:

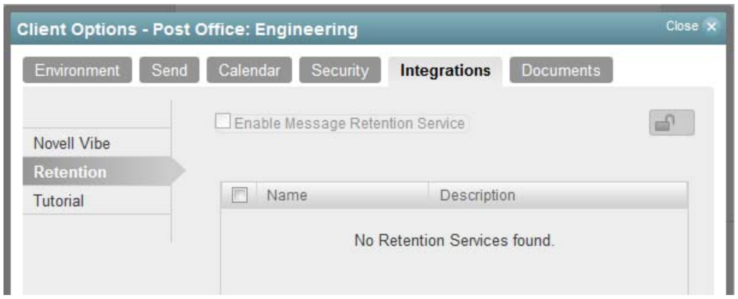
```
http://vibe_server:port_number/ssf/ws/TeamingServiceV1
```

Replace `vibe_server` with the base URL of the server where Micro Focus Vibe is running. If you are using the default port number, specifying `port_number` is optional. The remainder of the URL provides GroupWise with information it needs in order to display the Vibe site correctly within GroupWise

Integrations Options: Retention

The **Retention** tab is displayed only if the **Provides Message Retention Service** setting is selected for a trusted application. For information, see Chapter 50, “Retaining User Messages,” on page 429.

Message retention is configurable only by administrators, not by GroupWise users. The Retention options do not display in the GroupWise client.



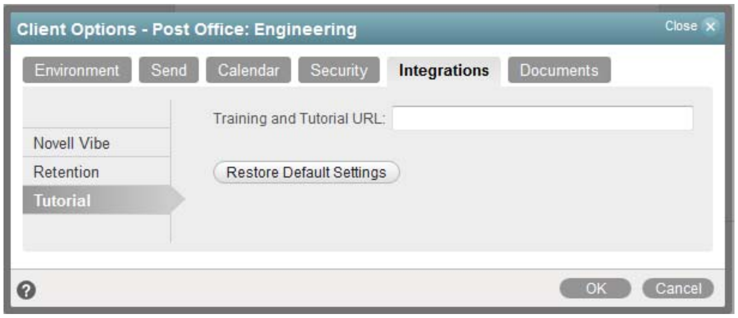
Enable Message Retention Service

Select this option to enable the Message Retention Service. If you are setting client options for a domain, all user mailboxes in the domain support message retention. Likewise, if you are setting options for a post office, all user mailboxes in the post office support message retention.

After a user’s mailbox is enabled for message retention, the user cannot perform any action (purging, archiving, etc.) that removes messages from the mailbox until the messages have been copied to another storage location by a trusted application that has been designed to provide the Message Retention Service.

Integrations Options: Tutorial

The Tutorial option provides the ability to change the URL that is displayed when the user clicks **Help > Training and Tutorials** in the GroupWise client.



Training and Tutorial URL

The default URL is:

http://www.brainstorminc.com/videos/gw18

If you purchase more in-depth training from BrainStorm, or you want to provide your own customized training materials for your GroupWise users, you can specify the URL that **Help > Training and Tutorials** displays in the GroupWise client.

Specify the URL for a custom training and tutorial web page.

Modifying Documents Options

1. In the GroupWise Admin console, display the Client Options **Documents** tab.

   For instructions, see Chapter 69, “Setting Defaults for the GroupWise Client Options,” on page 545.
2. Select the default library, then click **OK** to save your changes.

For information about libraries and document management, see Part XIII, “Libraries and Documents,” on page 511.

Resetting Client Options to Default Settings

You can reset client options to the defaults for one or more users. This enables you to establish your preferred settings, and then lock those settings so that users cannot change them in the future.

In the GroupWise Admin console:

1. To reset the client options of a single user, browse to and click the name of the user, then click **Maintenance**.

   or

   To reset the client options for multiple users:

   1a Browse to and click the name of the post office where the users are located.

   1b Click **Maintenance > Mailbox/Library Maintenance**.

   1c Select **Maintenance on Users/Resources in This Post Office**.

   1d Type a comma-separated list of user names.
2. In the **Actions** list, select **Reset Client Options**, then click **OK**.

70 Distributing the GroupWise Client

You can distribute the GroupWise client software in various ways:

- "Using Client Auto-Update to Distribute the GroupWise Client Software" on page 583
- "Using ZENworks Configuration Management to Distribute the GroupWise Client" on page 592

For information about client licensing requirements, see "Auditing Mailbox License Usage in the Post Office" on page 127.

Using Client Auto-Update to Distribute the GroupWise Client Software

The GroupWise Client Setup Wizard (`setup.exe`) includes a Client Auto-Update feature that helps you keep users' GroupWise client software up to date. Each time the GroupWise client starts, it checks with the POA for the user's post office to find out if new GroupWise client software is available in the post office. When new software is available and Client Auto-Update is enabled in the post office, the Setup program can prompt the user to install the updated software.

When you run the GroupWise Installation Wizard to install the GroupWise Server component, the GroupWise client software is installed in the following locations:

Linux:	`/opt/novell/groupwise/agents/data/client/setup/win32`
Windows:	`c:\Program Files\Micro Focus\GroupWise Server\agents\data\client\setup\win32`

Client Auto-Update is disabled by default. For a small GroupWise system, you can have the POA distribute the GroupWise client software. However, this represents an extra load on the POA whenever the GroupWise client software is updated and needs to be downloaded to users' workstations. A more robust solution is to configure your web server to distribute the GroupWise client software.

Using the POA to Distribution the GroupWise Client Software

- "Enabling Client Auto-Update for the POA" on page 583
- "Triggering a Client Update by the POA" on page 584

Enabling Client Auto-Update for the POA

You can configure Client Auto-Update at the domain, post office, or user level.

1 In the GroupWise Admin console, browse to and click the name of a domain, post office, or user.

2 Click **Client Options > Client Auto-Update**.

3 Select **Enable Client Auto-Update**.

4 Leave the **Auto-Update URL** field blank.

5 (Conditional) As needed, modify the update settings.
6 Click **OK**.
7 Create a new `win32` subfolder in the client software location for the `setup.cfg`.

   The Client Setup Wizard looks for the `setup.cfg` file in a `win32` subfolder relative to the location of the `setupip.fil` file.
8 Modify the setup configuration file (`setup.cfg`) used by the GroupWise Client Setup Wizard to customize the client installation process before you trigger the installation. Follow the steps in "Customizing the Setup Configuration File" on page 590 to modify the file.
9 Copy the setup.cfg file to the `/client/setup/win32/win32` folder that you created.
10 Continue with Triggering a Client Update by the POA.

Triggering a Client Update by the POA

Updates are triggered at the post office level.

1 Browse to and click the name of a post office where Client Auto-Update is enabled, either for all users in the post office or for individual users.
2 Click **More > Client Auto-Update**.
3 (Conditional) If you want to verify the update settings, click **Modify Settings** to go to the Post Office object **Client Auto-Update** tab, then return to the Client Auto-Update dialog box.
4 Click **Trigger Update**.
5 Skip to "Understanding the User's Client Auto-Update Experience" on page 592.

Using Your Web Server to Distribute the GroupWise Client Software

Configuring your web server to distribute the GroupWise client software frees the POA from this task. You must copy the GroupWise client software to a location on your web server from which it can be downloaded. Then you must configure your web server to allow downloads from the folder that you set up.

- "Setting Up the GroupWise Client Software on Your Web Server" on page 584
- "Enabling Client Auto-Update for Your Web Server" on page 586
- "Testing the Client Update from Your Web Server" on page 587
- "Triggering a Client Update from Your Web Server" on page 587

Setting Up the GroupWise Client Software on Your Web Server

Client Auto-Update can be configured to install the GroupWise client software from the Apache web server on Linux, or from the Internet Information Service (IIS) web server on Windows. Make sure you that you have a copy of the GroupWise client software available on your web server. For information on obtaining the GroupWise client software, see "Extracting the GroupWise Software" on page 536.

1 Create a folder in the document root folder of your web server for the GroupWise client software files used by Client Auto-Update, for example:

Apache on Linux:	`/srv/www/htdocs/gwclient/18.0.0`
IIS on Windows:	`c:\InetPub\wwwroot\gwclient\18.0.0`

2 Copy the contents of the `agents/data/client/setup/win32` folder that you created in “Extracting the GroupWise Software” on page 536 into the client software folder that you created in Step 1.

All language-independent GroupWise client software files are included in the `setupip.fil` file. The `setupip.`*`language_code`* file for each client language (`setupip.en`, `setupip.de`, `setupip.fr`, and so on) contains all client software files for the specific language indicated by the language code. If you have multiple `setupip.`*`language_code`* files on the web server, users are prompted for which languages they want to install.

3 (Conditional) If you do not want multiple language versions of the GroupWise client to be available to users, delete the language files that you do not need.

4 Create a new `win32` subfolder in the client software location for the `setup.cfg`.

The Client Setup Wizard looks for the `setup.cfg` file in a `win32` subfolder relative to the location of the `setupip.fil` file.

5 Modify the setup configuration file (`setup.cfg`) used by the GroupWise Client Setup Wizard to customize the client installation process before you trigger the installation. Follow the steps in “Customizing the Setup Configuration File” on page 590 to modify the file.

6 Copy the setup.cfg file to the `/win32` folder that you created.

7 Configure your web server to support Client Auto-Update:

- “Apache on Linux” on page 585
- “IIS on Windows Server” on page 586

Apache on Linux

1 Open the Apache configuration file (`/etc/apache2/httpd.conf`) in a text editor.

2 Search for the following section:

```
<Directory />
```

3 After the default `Directory` section, add the following section for the GroupWise client software:

```
<Directory /srv/www/htdocs/gwclient/18.0.0>
   Options Indexes
</Directory>
```

4 On the `Directory` line, specify the client software directory that you created in Step 1 in “Setting Up the GroupWise Client Software on Your Web Server” on page 584.

5 Save the file.

6 Restart Apache:

```
rcapache2 restart
```

7 Test the availability of the client software on the web server by displaying the following URL and verifying the contents of the `win32` directory:

```
http://web_server_address/gwclient/18.0.0
```

8 Continue with “Enabling Client Auto-Update for Your Web Server” on page 586.

IIS on Windows Server

1 On Windows Server, click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

2 Expand the Local Computer object, expand the Sites folder, expand your website, then select the client software directory that you created in Step 1 in "Setting Up the GroupWise Client Software on Your Web Server" on page 584.

3 Enable directory browsing so that the `gwclient` directory can be accessed:

3a In the Features View, double-click **Directory Browsing**.

3b In the **Actions** pane, click **Enable**.

3c Click the client software directory to return to the Features View.

4 Configure IIS to allow the download of the client software files:

4a In the Features View, double-click **MIME Types**.

4b In the **Actions** pane, click **Add**.

4c In the **File name extension** field, type `.*` (a period followed by an asterisk).

4d In the **MIME type** field, type `application/octet-stream`.

4e Click **OK**.

4f Click the client software directory to return to the Features View.

5 (Conditional) If you have configured file filtering at a higher level in this website, configure IIS to not filter out files in the client software directory:

5a In the Features View, double-click **Request Filtering**.

5b Click **Allow File Name Extension**.

5c In the **File name extension** field, type `.*` (a period followed by an asterisk).

5d Click **OK**.

6 Close IIS Manager.

7 Restart IIS:

7a Click **Start > Administrative Tools > Services**.

7b Right-click **World Wide Web Publishing Service**, then click **Restart**.

8 Test the availability of the client software on the web server by displaying the following URL and verifying the contents of the `win32` directory:

`http://`*`web_server_address/gwclient`*

9 In File Explorer, mark the `web.config` file as Hidden.

The `web.config` file is automatically created by IIS. It is not part of Client Auto-Update and causes an error if it is not hidden.

10 Continue with Enabling Client Auto-Update for Your Web Server.

Enabling Client Auto-Update for Your Web Server

You can configure Client Auto-Update at the domain, post office, or user level.

1 In the GroupWise Admin console, browse to and click the name of a domain, post office, or user.

2 Click **Client Options > Client Auto-Update**.

3 Select **Enable Client Auto-Update**.

4 Specify the URL where you have made the GroupWise client software available on your web server.
5 (Conditional) As needed, modify the update settings.
6 Click **OK**.
7 Continue with Testing the Client Update from Your Web Server.

Testing the Client Update from Your Web Server

Test the availability of the files in the *gwclient* folder on the web server by displaying the following URL and verifying the contents of the `win32` subfolder:

```
http://web_server_address/gwclient
```

Index of /gwclient/14.0.0

Name	Last modified	Size	Description
Parent Directory		-	
copyip.exe	31-Jan-2014 16:21	188K	
copyipen.dll	31-Jan-2014 16:22	7.0K	
setupip.en	01-Feb-2014 16:26	4.0M	
setupip.fil	01-Feb-2014 16:26	88M	
version.ini	31-Jan-2014 16:22	29	
win32/	01-Feb-2014 16:30	-	

When the `setupip.fil` file and `setupip.en` file are extracted on users' workstations prior to the client software installation, the files in the `win32` subfolder on the web server replace the standard files.

After checking the availability of the files, continue with "Triggering a Client Update from Your Web Server" on page 587.

Triggering a Client Update from Your Web Server

Updates are triggered at the post office level.

1 Browse to and click the name of a post office where Client Auto-Update is enabled, either for all users in the post office or for individual users.
2 Click **More > Client Auto-Update**.
3 (Conditional) If you want to verify the update settings, click **Modify Settings** to go to the Post Office object **Client Auto-Update** tab, then return to the Client Auto-Update dialog box.
4 Click **Trigger Update**.
5 Skip to "Understanding the User's Client Auto-Update Experience" on page 592.

Working with the Setup.cfg File

The installation of the GroupWise client software by the Client Setup Wizard is controlled by the setup configuration file (`setup.cfg`). The Client Auto-Update process can also make use of this file.

- "Understanding the Setup Configuration File (setup.cfg)" on page 588
- "Customizing the Setup Configuration File" on page 590
- "Adding LDAP Directory Service Accounts to the Setup Configuration File" on page 591

Understanding the Setup Configuration File (setup.cfg)

A default `setup.cfg` file is provided in the following folder:

`downloaded_groupwise_software_image``\client`

The `setup.cfg` file is an ASCII text file that supports extended ASCII characters. The file contains the responses that are normally provided by the user during the installation of the GroupWise client. For example, the path for the GroupWise client software and the folder for the GroupWise client desktop icon are specified in the `setup.cfg` file. In addition, information can be added to the `setup.cfg` to add predefined LDAP directory service accounts to the GroupWise Address Book in the GroupWise client during installation.

When the GroupWise Client Setup Wizard (`setup.exe`) is executed, it looks in the same folder for a `setup.cfg` file. If none is found, the installation proceeds, prompting the user for the needed information. If the `setup.cfg` file is found, the GroupWise Client Setup Wizard proceeds, using the information specified in the `setup.cfg` file. Depending on the entries in the `setup.cfg` file, the user might be prompted to provide information during the installation.

The `setup.cfg` file is divided into the following sections. In the `setup.cfg` file, each section head must be enclosed in brackets [ ] as shown.

- "[GroupWiseSetup]" on page 588
- "[ShowSetup]" on page 589
- "[Startup]" on page 589
- "[GWCheck]" on page 589
- "[Languages]" on page 590

[GroupWiseSetup]

`Version=`	This entry must match the version being installed; otherwise, the Setup Wizard does not use `setup.cfg`. The default is 18.0.
`Path=`	This entry specifies the path where you want the GroupWise client to be installed. The default path for GroupWise 18 is `c:\Program Files\Micro Focus\Groupwise`. GroupWise 8 and earlier defaulted to `c:\novell\groupwise`.
`Folder=`	This entry creates and installs the GroupWise client shortcuts to the specified folder in the user's **Start** menu. The default folder is Micro Focus GroupWise.
`LaunchMessenger=`	This optional entry specifies whether GroupWise Messenger should be launched when GroupWise starts. The default is `No`.
`LaunchNotify=`	This optional entry specifies whether GroupWise Notify should be launched when GroupWise starts. The default is `No`.
`OutlookFirewallException`	This entry specifies whether Outlook should be added to the Windows Firewall exceptions list. The default is `Yes` (add Outlook to the exceptions list).
`GWMailTo=`	This entry specifies whether the GroupWise client should be the default email application in your web browser. The default is `Yes`, so that the Internet Browser Mail Integration is installed along with the GroupWise client.

`IPAddress=`	This optional entry specifies the IP address for the GroupWise client to always use. Use this setting to set the IP address per post office when using multiple post offices.
`IPPort=`	This optional entry specifies the IP port for the GroupWise client to always use.
`DefaultIPAddress=`	This optional entry specifies the default IP address for the GroupWise client to use the first time it is started. This should be an IP address that everyone on the system has access to.
`DefaultIPPort=`	This optional entry specifies the default IP port for the GroupWise client to use the first time it is started.
`StopService=`	Use this entry when you are running integrated third-party software along with the GroupWise client, and that software might be locking some GroupWise client DLLs. If client DLLs are locked, the client software cannot be installed. Specify the service for the client Setup Wizard to stop before it installs the client software. Use the name as it appears in the list provided by **Control Panel > Administrative Tools > Services**. You can stop only one service before installing the client software.

[ShowSetup]

`ShowDialogs=`	Specify `No` to hide dialog boxes during the installation. Specify `Yes` to show the dialog boxes. The default is `Yes`. If an entry is missing from the `setup.cfg` file and `ShowDialogs=Yes`, the Setup Wizard selects the default setting. If `ShowDialogs=No`, the Setup Wizard prompts the user for a selection. **NOTE:** This option does not suppress the language selection dialog box that appears when you install the GroupWise client from the multilanguage software image. For more information, see “Unwanted Language Selection Dialog Box” in the GroupWise 18 Readme.
`ShowProgress=`	Specify `Yes` to show the progress indicator during the installation. Specify `No` to hide the progress indicator during installation. The default is `Yes`.
`ShowFinish=`	Specify `Yes` to display the Finish dialog box after the installation. Specify `No` to hide this dialog box. The default is `Yes`.

[Startup]

`Notify=`	If you specify `Yes`, the Setup Wizard places Notify in the Windows Startup folder to be started automatically when the computer starts. The default is `No`.

[GWCheck]

This section installs and enables GroupWise Check (GWCheck). GWCheck is a tool that performs maintenance and repair tasks on users’ mailboxes to keep GroupWise operating efficiently. It is essentially a standalone version of the Mailbox/Library Maintenance feature available in the

GroupWise Admin console. GWCheck checks and repairs GroupWise user, message, library, and resource databases independent from the Admin console. In addition to checking post office, user, and library databases, it also checks Caching, Remote, and archive databases.

`InstallGWCheck=`	Specify `Yes` to install GWCheck files to the workstation. Specify `No` to not install GWCheck. The default is `Yes`.
`GWCheckEnabled=`	Specify `Yes` to install the files to the same folder as the GroupWise client, which results in the **Repair Mailbox** option being enabled under the **Tools** menu in the GroupWise client. Specify `No` to install the files in a `GWCheck` subfolder below the `client` folder, which disables the **Repair Mailbox** option until the files are manually copied into the `GroupWise` folder. The default is `No`.

[Languages]

The default language is set to `English`, and all other languages are set to `No`, meaning they are not installed. See the `setup.cfg` file for a listing of the different languages.

Customizing the Setup Configuration File

1. On the server from which you want to distribute the GroupWise client software, browse to the following folder in the downloaded *GroupWise 18* software image:

   groupwise_software_image\client

2. Use an ASCII text editor to edit the copied `setup.cfg` file and add the settings that you want to use when Client Auto-Update installs the client software on users' workstations.

   To review the settings, see "Understanding the Setup Configuration File (setup.cfg)" on page 588.

   2a (Conditional) If you are installing multiple languages, but you do not want users to be prompted for the languages to install in the `[Startup]` section, specify:

   ```
   EnableLangDlg=No
   ```

3. Save the customized `setup.cfg` file.
4. (Optional) Continue with Adding LDAP Directory Service Accounts to the Setup Configuration File.
5. Return to the task of setting up Client Auto-Update:
   - "Enabling Client Auto-Update for the POA" on page 583
   - "Enabling Client Auto-Update for Your Web Server" on page 586

Adding LDAP Directory Service Accounts to the Setup Configuration File

LDAP directory service accounts provide users with the ability to search directory services such as Bigfoot for names and email addresses of people. Each search can check potentially millions of names. After locating a name through a directory service search, users can add those names and email addresses to their personal address books.

You can add predefined LDAP directory service accounts to the Address Book by adding information to `setup.cfg.` This information can be added even after the initial installation. After the accounts are added, this information does not need to be removed from `setup.cfg`. During subsequent installations, GroupWise adds any new accounts listed but does not update or duplicate existing LDAP accounts.

The user can also choose to add LDAP directory service accounts after the GroupWise client is installed. For more information, see "Using the LDAP Address Book" in the *GroupWise 18 Client User Guide*.

To add an LDAP address book during installation, add the following lines to the `setup.cfg` file, providing information that is specific to the LDAP account:

```
[LDAP Account 1]
Description=Ldap Server1
Server=ldap.server1.com
Port=389
SearchRoot=c=us
Login=TRUE
```

You can add multiple accounts:

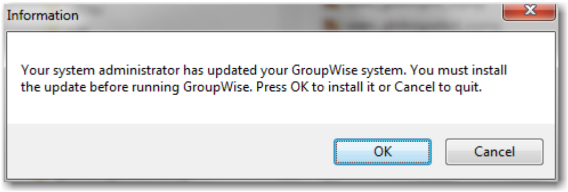
```
[LDAP Account 2]
Description=Ldap Server2
Server=ldap.server2.com
Port=389
SearchRoot=0=widget, c=us
Login=FALSE
```

Parameter	Description
`Description=`	The name that displays in the list of LDAP directory services in the Address Book.
`Server=`	The LDAP server name or IP address.
`Port=`	The LDAP directory service's port number. The number is usually 389.
`SearchRoot=`	The base or root of the LDAP directory service where the user searches for names. For example, the base could be a country, organization, or other type of grouping. This is not required for all LDAP directory services. If a search root is required, the LDAP directory service provides the information.
`Login=`	TRUE means users are prompted for a user name and password when they use that LDAP directory service.

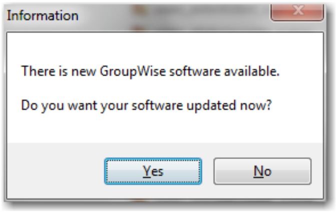
Understanding the User’s Client Auto-Update Experience

The next time each user starts the GroupWise client, the client detects that the software version in the post office has been updated. It launches the GroupWise Client Setup program (`setup.exe`), which runs according to the Client Auto-Update that settings you have provided.

If you are forcing the user to update, the following message appears:



If you are not forcing the user to update, the following message appears:



Using ZENworks Configuration Management to Distribute the GroupWise Client

You can use ZENworks Configuration Management to automatically distribute the GroupWise client software to users’ workstations. For instructions, see “Micro Focus ZENworks” in the *GroupWise 18 Interoperability Guide*.

71 Supporting the GroupWise Client in Multiple Languages

The GroupWise client software is available in a broad range of languages to meet the needs of users in many countries.

By installing the GroupWise client software in their language of choice, users can begin using GroupWise in that language immediately. However, some language-related details of GroupWise functionality are not taken care of by the client software running on users' workstations. Those aspect are affected by the language in use by the POA running for the post office to which users belong. The POA returns certain text in the language in which it is running, not the language in use on users' workstations.

- The status information (Delivered, Opened, an so on) displayed in the Properties page of items
- The text of return notification mail receipts (if the user has enabled this type of notification)
- The sort order in the GroupWise Address Book

In some circumstances, these issues can be resolved by grouping users who speak the same language into the same post office and then installing the POA in the same language that the users are using. For more information, see Chapter 12, "Creating a New Post Office," on page 119.

At present, the POA is available in fewer languages than the GroupWise client, so this solution helps only those client users who are somewhat familiar with the language in use by the POA. For more information, see Chapter 7, "Multilingual GroupWise Systems," on page 85.

72 Tools for Analyzing and Correcting GroupWise Client Problems

The following tools can assist you in analyzing and correcting GroupWise client problems.

GroupWise Exception Handler for the GroupWise Client

If the GroupWise client causes an exception (or “crashes”), GroupWise generates a GroupWise Exception Report. This report contains information that is useful in analyzing the problem that the client is having so that it can be solved.

The report is saved in `\temp\grpwise.rpt`. The `\temp` directory used is the one specified by the TMP environment variable, or if not defined by TMP, the one specified by the TEMP environment variable. If neither environment variable is defined, GroupWise uses the current the `windows` directory.

Each time an exception or crash occurs, a new report is appended to `grpwise.rpt`. If the file reaches 100 KB, the oldest reports (at the beginning of the file) are deleted.

The GroupWise Exception Report contains information such as the date and time the report was generated, the exception code, fault address, date of `grpwise.exe`, computer and user name where the exception occurred, hardware and operating system information, process modules, raw stack dumps, and call stacks.

GroupWise Check

GroupWise Check (GWCheck) is a tool that performs maintenance and repair tasks to keep GroupWise operating efficiently. It is essentially a standalone version of the Mailbox/Library Maintenance feature available in the GroupWise Admin console. GroupWise Check checks and repairs GroupWise user, message, library, and resource databases without needing the GroupWise Admin console. In addition to checking post office, user, and library databases, it also checks remote and archive databases.

GroupWise Check can be installed with the GroupWise client (unless you have specified in `setup.cfg` that it not be installed), and is available by clicking **Tools > Repair Mailbox** in the client in Caching and Remote modes after you complete the following:

1. Locate the directory named `gwcheck`. This is a subdirectory of the directory where the client is installed (usually `c:\Program Files\Micro Focus\GroupWise`).
2. Locate `grpwise.exe`. It is usually in `c:\Program Files\Micro Focus\GroupWise`.
3. Copy all the files in `gwcheck` to the directory where `grpwise.exe` is located.

You can now run GroupWise Check in Caching and Remote mode. The GroupWise Check dialog box is titled GroupWise Mailbox Maintenance. You can also use Ctrl+Shift when accessing a Caching or Remote mailbox to run GroupWise Check before opening the mailbox.

For detailed information about GroupWise Check, see “GroupWise Check” on page 433.

73 Startup Options for the GroupWise Client

The GroupWise client has optional startup options that you can use when you start the program. Some of these startup options are for your convenience, while others are necessary to run GroupWise on your particular hardware. For a complete listing, see “Startup Options” in the *GroupWise 18 Client User Guide*.

XV WebAccess

For a complete list of port numbers used by the WebAccess Application, see "WebAccess Application Port Numbers" on page 729.

For detailed Linux-specific WebAccess Application information, see Appendix C, "Linux Basics for GroupWise Administration," on page 735.

74 Accessing Your GroupWise Mailbox in a Web-Based Environment

GroupWise WebAccess consists of the WebAccess Application, which is installed to your web server, and the WebAccess user interface, where users work in their GroupWise mailboxes. WebAccess offers three different web-based environments for users. All three environments are made available when you install the WebAccess Application.

Using WebAccess on a Desktop Workstation

1 To access GroupWise WebAccess in a desktop browser, use the following URL:

   `http://web_server_address/gw/webacc`

   Replace *web_server_address* with the IP address or DNS hostname of your web server. If the web server uses SSL, use `https` rather than `http`.

2 Type your GroupWise user ID in the **User Name** box and your GroupWise mailbox password in the **Password** box.

3 (Optional) If you are in a secure location, select **This is a private computer**.

   On a private computer in a secure location, the default WebAccess timeout is 480 minutes (8 hours), which is convenient for day-long use. On a public or shared computer, the default timeout is 20 minutes, which protects your personal data. You can change these settings. For more information, see "Setting the Timeout Interval for Inactive WebAccess Sessions" on page 611.

4 (Optional) To change the WebAccess interface language, click **Options**, then select the language you want from the **Language** drop-down list.

5 Click **Login** to display the GroupWise WebAccess main window.

6 Click **Help** for more information about using GroupWise WebAccess.

Using WebAccess on a Tablet

1 To access GroupWise WebAccess on your tablet, use the following URL:

   `http://web_server_address/gw/webacc`

   Replace *web_server_address* with the IP address or DNS hostname of your web server. If the web server uses SSL, use `https` rather than `http`. The WebAccess Application detects that it is communicating with a tablet and provides the WebAccess Mobile interface.

   or

   (Conditional) If you have a tablet that is not yet supported, but you want to see how well the mobile interface works on your device, use the following URL:

   `http://web_server_address/gw/webacc?User.interface=mobile`

2 Type your GroupWise user name in the **User Name** box and your GroupWise mailbox password in the **Password** box.

3 (Optional) To change the WebAccess interface language, click **Settings**, then select the language you want from the **Language** drop-down list.

4 Click **Login** to display the GroupWise WebAccess main window on your tablet.

5 Click **More > Help** for more information about using GroupWise WebAccess on your tablet.

Using the WebAccess Basic Interface on a Mobile Device

1 To access GroupWise WebAccess in the web browser on your mobile device such as a cell phone, use the following URL:

```
http://web_server_address/gw/webacc
```

Replace *web_server_address* with the IP address or DNS hostname of your web server. If the web server uses SSL, use `https` rather than `http`. The WebAccess Application detects that it is communicating with a mobile device such as a cell phone and provides the WebAccess basic interface.

2 Enter your GroupWise user ID and GroupWise mailbox ID.

The appearance of the WebAccess basic interface varies, depending on the size of the screen where it is displayed.

3 For more information about using WebAccess on your mobile device, see the *WebAccess Basic Interface Quick Start* (http://www.novell.com/documentation/groupwise18/gw18_qs_webaccbasic/data/gw18_qs_webaccbasic.html).

4 Follow the instructions in your mobile device's documentation to add this URL to your Favorites or Bookmarks so you don't need to type the URL every time you log in on your mobile device.

As an alternative to this limited interface, you can synchronize GroupWise data to your mobile device using the GroupWise Mobility Service. For more information, see the GroupWise Mobility Service Documentation website (http://www.novell.com/documentation/groupwisemobility2).

75 Scaling Your GroupWise WebAccess Installation

If your GroupWise system is relatively small (one domain and a few post offices) and all post offices reside in the same location, installing the GroupWise WebAccess Application on one web server might meet your needs. However, if your GroupWise system is large, spans multiple locations, or requires failover support, you might need to install the WebAccess Application on multiple web servers to meet the reliability, performance, and availability needs of your GroupWise WebAccess users.

The following sections provide information about the various configurations you can implement and instructions to help you create the configuration you choose.

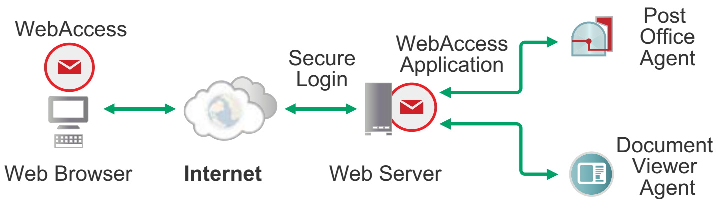
For information about installing the initial instance of the WebAccess Application, see "Setting Up GroupWise WebAccess" in the *GroupWise 18 Installation Guide*.

WebAccess Configurations

Depending on the needs of your GroupWise system, it might be necessary for you to have multiple web servers running the WebAccess Application.

Basic WebAccess Application Installation

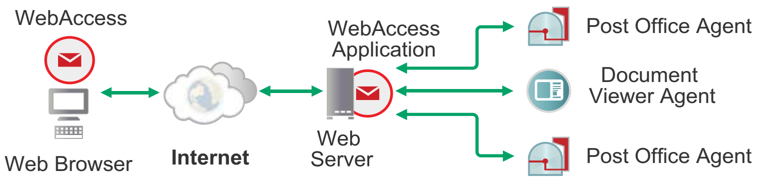
A basic installation of GroupWise WebAccess requires the WebAccess Application, a POA, and a DVA, as shown in the following diagram.



Multiple POAs for a WebAccess Application

When you install the WebAccess Application, you configure it to communicate with a single POA. However, in this simple configuration, if that POA goes down, WebAccess users cannot access their mailboxes, even if all other the POAs in your GroupWise system are still running.

Configuring the WebAccess Application for multiple POAs provides more stable access. Three POAs are recommended, but there is no limit to the number of POAs that you can configure the WebAccess Application to communicate with. When a POA stops responding, the WebAccess Application contacts the next POA in the list to provide uninterrupted access (except, of course, for the users whose mailboxes are in the post office where the POA is down).

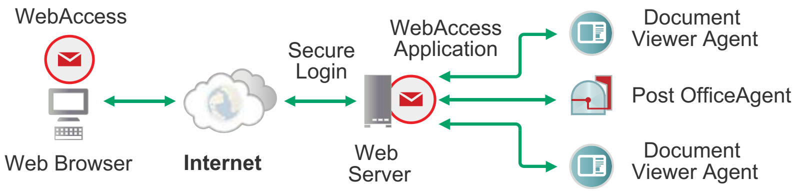


For setup instructions, see “Configuring the WebAccess Application with Multiple POAs for Fault Tolerance” on page 608.

Multiple DVAs for a WebAccess Application

When you install the WebAccess Application, you configure it to communicate with a single DVA. Again, in this simple configuration, if that DVA goes down, no WebAccess users can view attached documents until that DVA is running again.

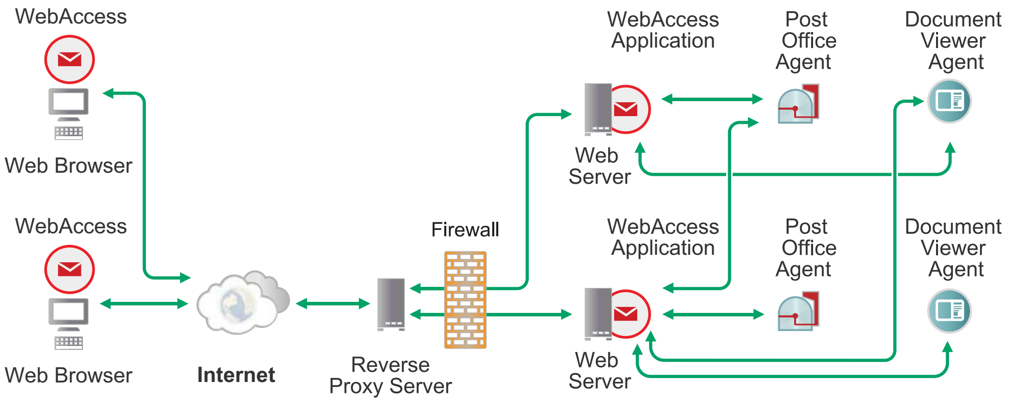
Configuring the WebAccess Application for multiple DVAs provides more reliable document conversion. Three DVAs are recommended, but there is no limit to the number of DVAs that you can configure the WebAccess Application to communicate with. When a DVA stops responding, the WebAccess Application contacts the next DVA in the list to provide uninterrupted document conversion.



For setup instructions, see “Configuring WebAccess Application with Multiple DVAs for Attachment Viewing” on page 609.

Multiple WebAccess Applications and Web Servers for a Large WebAccess Installation

In a larger GroupWise system, you can install the WebAccess Application to multiple web servers.



There are various reasons why you might want to add additional WebAccess Applications, including:

- **Improving WebAccess reliability:** One WebAccess Application might provide sufficient access and performance, but you want to protect against downtime that would occur if the WebAccess Application became unavailable because of web server failure or some other reason. Installing more than one WebAccess Application enables you to set up failover support to make your system more reliable.
- **Improving WebAccess performance:** The WebAccess Application is designed to be close to GroupWise post offices. It requires SOAP access to the POAs. For best performance, you should ensure that the WebAccess Application is on the same local area network as the POA that it communicates with. For example, in most cases you do not want a WebAccess Application in Los Angeles communicating with a POA in London.
- **Improving WebAccess availability:** Adding additional WebAccess Applications enables GroupWise WebAccess users on an intranet to access GroupWise through an internal web server and WebAccess users on the Internet to access GroupWise through an exposed web server.
- **Improving web server performance:** Adding additional WebAccess Applications increases web server performance by balancing the workload among several web servers, especially if you are using the web server for other purposes in addition to GroupWise WebAccess.

WebAccess Installation on Additional Web Servers

On each web server where you want to install the WebAccess Application, follow the instructions in "Setting Up GroupWise WebAccess" in the *GroupWise 18 Installation Guide*.

When you have multiple WebAccess Applications for your GroupWise system, its recommended to have a Layer 4 Switch in front of the two or more WebAccess Application web servers. Select a friendly hostname such as `gwmail.yourcompanyname.com` that users can type in their web browsers. Set up a DNS redirection so that `gwmail.yourcompanyname.com` automatically redirects to `https://gwmail.yourcompanyname.com/gw/webacc`, and when the WebAccess Application on that main web server communicates with a POA, it then redirects the WebAccess user to the proper post office and POA for mailbox access.

76 Configuring the WebAccess Application

For WebAccess system requirements, see "GroupWise WebAccess System Requirements" in the *GroupWise 18 Installation Guide*. For detailed instructions about installing and setting up the WebAccess Application for the first time, see "Setting Up GroupWise WebAccess" in the *GroupWise 18 Installation Guide*.

The default configuration of WebAccess is adequate for users to start accessing their GroupWise mailboxes from web browsers. You can customize the WebAccess configuration to meet the specific needs of you and your GroupWise users by editing the `webacc.cfg` file.

- "Customizing the WebAccess Application" on page 607
  - Editing the webacc.cfg File
  - Configuring the WebAccess Application with Multiple POAs for Fault Tolerance
  - Configuring WebAccess Application with Multiple DVAs for Attachment Viewing
  - Disabling Caching of Attachments
  - Adjusting Session Security
  - Accommodating Single Sign-On Products
- "Managing User Access" on page 611
  - Setting the Timeout Interval for Inactive WebAccess Sessions
  - Customizing Auto-Save Functionality
  - Preventing Users from Changing Their GroupWise Passwords in WebAccess
  - Helping Users Who Forget Their GroupWise Passwords
  - Controlling WebAccess Usage
- "Customizing User Functionality" on page 615
  - Customizing the WebAccess User Interface with Your Company Logo
  - Controlling the WebAccess New Item Notification Sound
  - Customizing Auto-Refresh Functionality
  - Controlling Viewable Attachment Types
  - Controlling Viewable Attachment Size
  - Customizing the Default Calendar View
  - Customizing the Default List Functionality
  - Enabling an LDAP Address Book

Customizing the WebAccess Application

The WebAccess Application, which resides on the web server, provides the GroupWise WebAccess user interface. As users perform actions in GroupWise WebAccess, the WebAccess Application passes information between the web browser, the POA, and the DVA.

During installation, the WebAccess Application is set up with a default configuration in the `webacc.cfg` file. You can modify the WebAccess Application configuration to meet the needs of your WebAccess users and your administrator preferences.

Editing the webacc.cfg File

The location of the `webacc.cfg` file varies by platform:

Linux:	`/var/opt/novell/groupwise/webaccess`
Windows:	`c:\Micro Focus\GroupWise\webaccess`

You can use any ASCII text edit that you prefer to edit the `webacc.cfg` file.

IMPORTANT: We strongly recommend that you do not modify any settings that are not documented in the following sections.

Configuring the WebAccess Application with Multiple POAs for Fault Tolerance

When you install the WebAccess Application, you configure it to communicate with a single POA. After installation, you can configure the WebAccess Application to communicate with multiple POAs. There is no limit to the number of POAs you can specify. Three POAs is recommended. The POAs you specify must be configured for SOAP.

If the POA that the WebAccess Application is communicating with becomes unavailable, the WebAccess Application contacts the next POA in the list, providing uninterrupted service for WebAccess users.

To specify additional POAs:

1 Open the `webacc.cfg` file in a text editor.

2 Search to find the following lines:

```
Provider.SOAP.1.ip=
Provider.SOAP.1.port=
```

These lines identify the POA that you specified during installation.

3 Copy and paste those two lines, replace 1 with 2, then specify the IP address and SOAP port of a another POA, for example:

```
Provider.SOAP.2.ip=172.16.5.18
Provider.SOAP.2.port=7191
```

4 Repeat Step 3, incrementing the number, and providing the IP addresses and SOAP ports for additional POAs as needed.

5 Save the `webacc.cfg` file.

6 Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Configuring WebAccess Application with Multiple DVAs for Attachment Viewing

When you install the WebAccess Application, you configure it to communicate with a single DVA. After installation, you can configure the WebAccess Application to communicate with multiple DVAs. There is no limit to the number of DVAs you can specify. Three DVAs is recommended.

If the DVA that the WebAccess Application is communicating with becomes unavailable, the WebAccess Application contacts the next DVA in the list, providing uninterrupted document conversion for viewing attachments in HTML format.

To specify additional DVAs:

1. Open the `webacc.cfg` file in a text editor.
2. Search to find the following lines:

   ```
   Provider.DVA.1.ip=
   Provider.DVA.1.port=
   ```

   These lines identify the DVA that you specified during installation.
3. Copy and paste those two lines, replace 1 with 2, then specify the IP address and SOAP port of a another DVA, for example:

   ```
   Provider.DVA.2.ip=172.17.5.18
   Provider.DVA.2.port=8301
   ```

4. Repeat Step 3, incrementing the number, and providing the IP addresses and SOAP ports for additional DVAs as needed.
5. Save the `webacc.cfg` file.
6. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Disabling Caching of Attachments

When viewing attachments using WebAccess, the attachments are cached on your device by default. You can disable caching of viewed attachments in the `webacc.cfg` file:

1. In the `webacc.cfg` file, search for the following lines:
   - **Templates.Interface.1.disableCache:** Controls caching of attachments on PCs.
   - **Templates.Interface.2.disableCache:** Controls caching of attachments on smart phones.
   - **Templates.Interface.3.disableCache:** Controls caching of attachments on tablet devices.
2. Change `false` to `true` for the devices on which you don't want to cache attachments.
3. Save the `webacc.cfg` file.
4. Continue with "Putting WebAccess Configuration Changes into Effect" on page 610.

Adjusting Session Security

By default, the WebAccess Application uses the web browser IP address of the WebAccess user to confirm that, during the same session, it is always communicating with the same user. This is the highest form of security and works well for users on desktop workstations. However, for laptops and mobile devices that are carried to different places, possibly from one network segment to another, this level of security can cause interruptions in user sessions.

Other WebAccess Application security features, such as session cookies, provide excellent security, even without the IP address checking. If you have a large number of mobile WebAccess users, you can turn off the web browser IP address confirmation to make WebAccess more stable for these mobile users.

To disable IP address checking:

1 Open the `webacc.cfg` file in a text editor.

2 Search to find the following line:

```
Security.UseClientIP.enable=
```

3 Change `true` to `false`.

4 Save the `webacc.cfg` file.

5 Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Accommodating Single Sign-On Products

Some organizations choose to place a single sign-on product such as NetIQ Access Manager (https://www.netiq.com/products/access-manager/) between users on the web and the applications they access that are running behind the organization's firewall. If you use a single sign-on product with WebAccess, you must configure the WebAccess Application to accommodate the single sign-on product.

1 Open the `webacc.cfg` file in a text editor.

2 Search to find the following line:

```
#Cookie.domain=.novell.com
```

3 Remove the pound sign (#) to activate the setting.

4 Replace `.novell.com` with the part of your organization's Internet domain name that is common between the single sign-on product and the web server where the WebAccess Application is installed.

   For example, if the Access Manager server is at `nam.novell.com` and the WebAccess Application is at `webacc.novell.com`, the domain name used to create cookies would be `.novell.com`, so that the cookies are accepted by both servers.

5 Save the `webacc.cfg` file.

6 Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Putting WebAccess Configuration Changes into Effect

- "Accepting the Default Time Interval" on page 611
- "Changing the Default Time Interval" on page 611
- "Immediately Putting the Configuration Changes into Effect" on page 611

Accepting the Default Time Interval

By default, the WebAccess Application checks the `webacc.cfg` file and the `gwac.xml` file for changes every 10 minutes. When it finds changes, it puts the changes into effect without restarting Tomcat. If you are satisfied with having your changes put into effect within this time interval, no action is required on your part after you edit the `webacc.cfg` file or the `gwac.xml` file.

Changing the Default Time Interval

You can change the time interval at which the WebAccess Application checks the `webacc.cfg` file and the `gwac.xml` file for changes.

1 Open the `webacc.cfg` file in a text editor.

2 Search to find the following line:

```
Config.Update.check=10
```

3 Change `10` to the number of minutes you want the WebAccess Application to wait before checking for changes to its configuration file.

4 Save the `webacc.cfg` file.

Immediately Putting the Configuration Changes into Effect

You can also manually restart Tomcat in order to put the changes into effect immediately.

SLES:	`rcgrpwise-tomcat8 stop rcgrpwise-tomcat8 start`
Windows:	1. At the Windows server, click **Start** > **Administrative Tools** > **Services**. 2. Right-click **Tomcat 8**, then click **Restart**.

Managing User Access

Setting the Timeout Interval for Inactive WebAccess Sessions

Users are eventually logged out of GroupWise WebAccess if they have not performed any actions that generate requests. Actions such as opening or sending a message generate requests. Other actions, such as scrolling through the Item List, composing a mail message without sending it, and reading Help topics, do not generate requests.

The timeout interval depends on whether the user selects **This is a public or shared computer** or **This is a private computer** in the Login window. On a private computer in a secure location, the default WebAccess timeout is 480 minutes (8 hours), which is convenient for day-long use. On a public or shared computer, the default timeout is 20 minutes, which protects your personal data. The timeout interval provides security for GroupWise WebAccess users who forget to log out. It also helps the performance of the web server by freeing the resources dedicated to that user’s connection.

The WebAccess Application on the web server controls the timeout. At the time the user is logged out, the WebAccess Application saves the user’s current session to a folder on the web server, where it is stored for 24 hours. If the logged-out user attempts to continue the session, he or she is prompted to log in again, after which the WebAccess Application renews the session. For example, suppose a

user is composing a message when the timeout interval expires and then attempts to send the message. The user is prompted to log in again, after which the message is sent. No information is lost.

To adjust the timeout interval:

1. Open the webacc.cfg file in a text editor.
2. To change the timeout interval for use on a public or shared computer, search to find the following line:

   ```
   Security.timeout=20
   ```

3. Change the default of `20` to the number of minutes that you prefer for the public/shared timeout interval.
4. To change the timeout interval for use on a private computer, search to find the following line:

   ```
   Security.Private.timeout=480
   ```

5. Change the default of 480 to the number of minutes that you prefer for the private timeout interval.
6. Save the `webacc.cfg` file.
7. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

The timeout interval applies to all users who log in through the web server where the WebAccess Application is running. You cannot set individual user timeout intervals. However, if you have multiple web servers, you can set different timeout intervals for the web servers by completing the above steps for each server's WebAccess Application.

Customizing Auto-Save Functionality

By default, GroupWise WebAccess automatically saves users' work on a regular basis, so that if a problem with a web server occurs or the user times out, their work is not lost. For details about the Auto-Save feature, see "Saving Unfinished Email" in the *GroupWise 18 WebAccess User Guide*.

Increasing the settings so that users' work is saved less frequently reduces the load on the web server but increases the amount of work that users could potentially lose. Reducing the settings so that users' work is saved more frequently increases the load on the web server, but reduces the amount of work that users could potentially lose.

To adjust the Auto-Save intervals:

1. Open the webacc.cfg file in a text editor.
2. Search to find the `Auto Save` section.
3. For the `Autosave.NonUse.timer` setting, increase or decrease the number of seconds after which the content is saved if there have been no modifications since the last save.

   The default non-use interval is 10 seconds. Specify 0 (zero) to turn off this functionality.
4. For the `Autosave.Use.timer` setting, increase or decrease the number of seconds after which the content is saved even when users are actively composing content.

   The default is 60 seconds. Specify 0 (zero) to turn off this functionality.
5. Save the `webacc.cfg` file.
6. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Preventing Users from Changing Their GroupWise Passwords in WebAccess

By default, users are allowed to change their GroupWise passwords in WebAccess. You can prevent them from doing so if you prefer that users change their passwords in some other way, for example if you are using an LDAP directory for authentication.

To adjust password security:

1. Open the `webacc.cfg` file in a text editor.
2. Search to find the following line:

   ```
   User.Access.security
   ```

3. Change `true` to `false`.
4. Save the `webacc.cfg` file.
5. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Helping Users Who Forget Their GroupWise Passwords

The GroupWise WebAccess Login page provides a **Can't log in** link for users to click when they have forgotten their GroupWise passwords. By default, the link displays the following file:

`/var/opt/novell/tomcat8/webapps/gw/webaccess/`*`yyyymmddnnnn`*`/images/helpdesk.htm`

The variable *yyyymmddnnnn* represents the year, month, day, and build number of the WebAccess software that you have installed.

You can use your HTML editor of choice to customize the contents of this file. For example, you might want to include the email address of the local GroupWise administrator who handles password issues, or perhaps the URL of your company's Help Desk web page.

As an alternative, you can configure the WebAccess Application to display any URL of your choosing.

1. Open the `webacc.cfg` file in a text editor.
2. Search to find the following line:

   ```
   #Helpdesk.url=http://www.novell.com/helpdesk.html
   ```

3. Remove the pound sign (#) to activate the setting.
4. Replace the sample URL with wherever you want users to be directed when they have forgotten their GroupWise passwords.
5. Save the `webacc.cfg` file.
6. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Controlling WebAccess Usage

You can control which users can use WebAccess to access their GroupWise mailboxes. By default, all GroupWise users can use WebAccess.

You can control access based on the domain or post office where the user's mailbox is located. You can control access for related users based on groups, and you can control access for individual users.

Access control is established through the `gwac.xml` file, located in the same folder with the `webacc.cfg` file.

The default `gwac.xml` file illustrates the following options:

```
<!-- To allow access to all EXCEPT a few, use this technique. -->
<!--
<gwac access="prevent">
  <domain name="domain1" />
  <postOffice name="po2.domain2" />
  <user name="jdoe.po3.domain3" />
  <distributionList name="helpdesk.po4.domain4" />
  <resource name="confroom.po4.domain4" />
</gwac>
-->

<!-- To prevent access to all EXCEPT a few, use this technique -->
<!--
 <gwac access="allow">
  <domain name="domain1" />
  <postOffice name="po2.domain2" />
  <user name="jdoe.po3.domain3" />
  <distributionList name="helpdesk.po4.domain4" />
  <resource name="confroom.po4.domain4" />
</gwac>
-->
```

You can use any ASCII text editor that you prefer to edit the `gwac.xml` file.

1. Open the `gwac.xml` file in a text editor.

   Typically, you use the `gwac.xml` file to override the default of allowing all users to use WebAccess.

2. Remove the comment marker lines (`<!--` and `-->`) around the section that you want to use.

3. (Optional) Under the `<gwac access="prevent">` line, create one or more lines to prevent users in one or more domains from using WebAccess, for example:

   ```
   <domain name="provo5"/>
   <domain name="provo6"/>
   ```

4. (Optional) Create one or more lines to prevent users in one or more post offices from using WebAccess, for example:

   ```
   <postOffice name="interns.provo1"/>
   <postOffice name="temps.provo1"/>
   ```

   Specify the post office in *post_office.domain* format.

5. (Optional) Create one or more lines to prevent users in one or more groups from using WebAccess, for example:

   ```
   <distributionList name="webaccessdenied.admin.provo1"/>
   ```

   Specify the group in *group.post_office.domain* format.

   Using one or more groups is the most flexible approach to access control for WebAccess. The group belongs to a specific post office (for example, the one you belong to), but it can include GroupWise users located anywhere in your GroupWise system. By using a group, you can easily modify access control for specific users by modifying the group in the GroupWise Admin

console, rather than needed to modify the gwac.xml file whenever access control changes are needed. For more information about groups, see Chapter 56, “Creating and Managing Groups,” on page 485.

6 (Optional) Create one or more lines to prevent specific users from using WebAccess, for example:

```
<user name="sjones.interns.provo1"/>
<user name="gbock.interns.provo1"/>
```

7 (Conditional) If you want to prevent most users and allow only specified users, use a `<gwac access="allow">` line instead of a `<gwac access="prevent">` line.

8 Save the gwac.xml file.

9 Skip to “Putting WebAccess Configuration Changes into Effect” on page 610.

Customizing User Functionality

You can control the functionality of certain aspects of the GroupWise WebAccess user interface. Any changes you make take effect the next time users log in to WebAccess.

Customizing the WebAccess User Interface with Your Company Logo

You can customize the WebAccess user interface to display your company logo. Interface customizations are established through the customization.cfg file, which is located in the same folder as the webacc.cfg file. The logo size for the WebAccess Login window must not exceed 215 pixels in width by 120 pixels in height.

1 Ensure that you have company logo that approximately match the size and shape of the Micro Focus logo that you are replacing.

2 Copy the logo image file to a location on your web server where it can be displayed by specifying a URL.

The logo image file must reside on the same server with the WebAccess Application that you are configuring. You can put it in a subfolder under your web server’s document root folder.

3 Open the customization.cfg file in a text editor.

4 Specify the logo image to use in the WebAccess Login window:

4a Uncomment the following line:

```
Company.Logo.Login.src=
```

4b Replace the sample URL with the URL for the company logo file for the Login window.

4c Replace the sample mouse-over text with the mouse-over text for your company logo.

5 Save the customization.cfg file.

6 Skip to “Putting WebAccess Configuration Changes into Effect” on page 610.

Controlling the WebAccess New Item Notification Sound

- “Customizing the New Item Notification Sound” on page 616
- “Turning Off the New Item Notification Sound” on page 616

Customizing the New Item Notification Sound

You can customize the sound that WebAccess users hear when a new item arrives in their GroupWise Mailbox. The default sound file is named `notifyClient.wav`.

1. Copy the desired sound file to a location on your web server where it can be played by specifying a URL.

   The sound file must reside on the same server with the WebAccess Application that you are configuring. You can put it in a subfolder under your web server's document root folder.
2. Open the `webacc.cfg` file in a text editor.
3. Search to find the following line:

   ```
   Notification.NewMail.sound=
   ```
4. Replace the default URL with the URL for the desired sound file.
5. Save the `webacc.cfg` file.
6. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Turning Off the New Item Notification Sound

1. Open the `webacc.cfg` file in a text editor.
2. Search to find the following line:

   ```
   Notification.enabled=true
   ```
3. Change `true` to `false`.
4. Save the `webacc.cfg` file.
5. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Customizing Auto-Refresh Functionality

WebAccess automatically refreshes users' web browsers so that the current contents of their mailboxes are always displayed.

By default, WebAccess uses 5 threads for polling, with a maximum of 20 threads allowed, and polling takes place on port 8500.

By default, WebAccess starts actively polling for updates from the POA after 10 minutes of inactivity, and keeps checking every minute until it is contacted by the POA

You can change these behaviors as needed.

1. Open the `webacc.cfg` file in a text editor.
2. Search to find the following lines:

   ```
   #SOAP.Poll.port=8500
   #SOAP.Poll.Threads.default=5
   #SOAP.Poll.Threads.max=20
   ```
3. Remove the pound sign (#) to activate the setting.
4. Adjust a poll settings as needed for your WebAccess users.

5 Search to find the following lines:

```
Poll.Idle.timeout=10
Poll.Idle.interval=1
```

6 Save the `webacc.cfg` file.

7 Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Controlling Viewable Attachment Types

By default, WebAccess allows users to view attachments in their native file formats for all file extensions except `.rar` (Roshall Archive, a compressed archive format) and `.avi` (Audio Visual Interleaf format). For all other file types, the **View** link is available in WebAccess. You can configure the WebAccess Application so that the **View** link is not available for additional file types.

To add to the list of file types that WebAccess users cannot view in native file format:

1 Open the `webacc.cfg` file in a text editor.

2 Search to find the following line:

```
Document.View.excludeDocExtensions=
```

3 Add file extensions to the list, separating each file extension with a comma.

Do not include periods on the file extensions or spaces between the file extensions.

4 Save the `webacc.cfg` file.

5 Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Controlling Viewable Attachment Size

By default, users can view allowable attachment types that are less than 1 MB is size. Increasing the maximum viewable attachment size increases the load on the web server. Decreasing the maximum viewable attachment size decreases the load on the web server.

For allowable attachment types that do not exceed the size limit, the **View** link is available in WebAccess. For allowable attachment types that exceed the size limit, the **View** link is not available, and users must save the large attachments in order to view them.

To adjust the viewable attachment size limit:

1 Open the `webacc.cfg` file in a text editor.

2 Search to find the following line:

```
Document.View.maxSize=
```

3 Increase or decrease the size as needed.

Specify the size in bytes. For example, 1024000 is 1 MB.

4 Save the `webacc.cfg` file.

5 Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Customizing the Default Calendar View

By default, WebAccess displays the Week view of the calendar.

You can change the default to the Day view.

Or you can change the default to the month view.

The default you select affects how the Calendar displays for GroupWise users to access their mailboxes through this instance of the WebAccess Application.

To change the default Calendar view:

1. Open the `webacc.cfg` file in a text editor.
2. Search to find the following line:

   `User.Calendar.defaultView=`

3. Change `Week` to `Day` or `Month`.
4. Save the `webacc.cfg` file.
5. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Customizing the Default List Functionality

By default, in lists of items, contacts, and Find results, GroupWise WebAccess users can Shift+click and Ctrl+click to select multiple items to perform an action on.

Some web-based interfaces use check boxes for multiple selection. This interface option is also available for GroupWise WebAccess.

To configure WebAccess to display check boxes:

1. Open the `webacc.cfg` file in a text editor.
2. Search to find the following line:

   `List.Checkboxes.show=`

3. Change `false` to `true`.
4. Save the `webacc.cfg` file.
5. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Customizing New Item Handling for Tablet Users

By default, WebAccess Mobile previews the first unread message when the user logs in. You can configure WebAccess Mobile to open the first unread message rather than previewing it, if that is more convenient for users.

1. Open the `webacc.cfg` file in a text editor.
2. Search to find the following line:

   `Mobile.Interface.UnreadItem.showMessagePreview=true`

3. Change `true` to `false`.
4. Save the `webacc.cfg` file.
5. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Enabling an LDAP Address Book

You can configure WebAccess to access an LDAP directory as if it is a GroupWise address book.

1 Open the `webacc.cfg` file in a text editor.

2 Search to find the following line:

```
User.Access.LDAP=false
```

3 Change `false` to `true` to enable users to access an LDAP address book.

4 Save the `webacc.cfg` file.

5 Open the `ldap.cfg` file in a text editor.

6 Replace the sample information in the `ldap.cfg` file with the specific information for the LDAP directory that you want users to access as a GroupWise address book.

7 Save the `ldap.cfg` file.

8 Follow the instructions in "Putting WebAccess Configuration Changes into Effect" on page 610.

9 Verify that the LDAP directory is available as a GroupWise address book:

   9a In WebAccess, open a new item.

   9b Click **Address**, then click the **Plus** icon.

   9c Expand the list of address books, then select the LDAP address book.

10 (Conditional) If the LDAP address book does not appear in the list:

   10a Check your modifications to the `webacc.cfg` file and `ldap.cfg` file for errors.

   10b Check the WebAccess Application log file for error messages.

   For assistance, see "Using WebAccess Application Log Files" on page 621.

   10c Resolve the problem, so that the LDAP address book appears in the list of address books.

11 Verify that the LDAP address book works as expected:

   11a Send a message to a recipient in the LDAP address book.

   11b Verify that the message was delivered successfully.

12 Notify GroupWise users that the LDAP address book is available, and explain to them how to access it.

The LDAP address book is available only in the Address Selector and only in WebAccess. It is not available in the GroupWise client.

77 Monitoring the WebAccess Application

The WebAccess Application can be monitored in your web browser. You can also use log files to monitor the WebAccess Application.

Using the WebAccess Application Console

The WebAccess Application includes a console that you can use to monitor it. The console lets you see information about logged-in users, such as their IP address, their GroupWise and web browser versions. In addition, you can view the WebAccess Application's log files and configuration files. The WebAccess Application console is disabled by default.

Enabling the WebAccess Application Console

1. Open the `webacc.cfg` file in a text editor.
2. Search to find the `Application Administration Tool` section.
3. For the `Admin.WebConsole.enable` setting, change `false` to `true`.
4. Save the `webacc.cfg` file.
5. Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Using the WebAccess Application Console

1. In a web browser, enter the following URL:

   `http://`*`server_address`*`/gw/webacc?action=Admin.Open`

   Replace `server_address` with the web server's IP address or DNS hostname.
2. When prompted, enter the GroupWise Admin user name and password.

   The console is displayed.

Using WebAccess Application Log Files

Error messages and other information about WebAccess Application functioning are written to log files as well as displaying on the WebAccess Application server console (Windows only). Log files can provide a wealth of information for resolving problems with WebAccess Application functioning or message flow. Logging is enabled by default.

Locating WebAccess Application Log Files

By default, WebAccess Application log files (*mmdd*`was.`*nnn*) are located in the following folders:

Linux:	`/var/opt/novell/groupwise/webaccess/logs`
Windows:	`c:\novell\groupwise\webaccess\logs`

You can change the location where the WebAccess Application creates its log files. For more information, see "Configuring WebAccess Application Log Settings" on page 622.

Configuring WebAccess Application Log Settings

1 Open the `webacc.cfg` file in a text editor.

2 Search to find the `Logging Information` section.

3 Adjust the following log settings as needed:

   Log.maxSize: Specify the maximum amount of disk space you want to use for WebAccess Application log files. If the disk space limit is exceeded, the WebAccess Application deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 102400 KB (100 MB).

   Log.maxAge: Specify the number of days you want to retain the log files. The WebAccess Application retains log files for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 30 days.

   Log.level: There are three log levels:

   - **Normal (default)** Displays warnings and errors.
   - **Verbose:** Displays the Normal log level information, plus information messages and user requests.
   - **Diagnostic:** Displays all possible information. Use Diagnostic only if you are troubleshooting a problem with the WebAccess Application.

     The Verbose and Diagnostic log levels do not degrade WebAccess Application performance, but log files consume more disk space when Verbose or Diagnostic logging is in use.

   Log.path: Specify the file path where you would like the log files to be stored. For example:

   ```
   Log.path=C:/User/jdoe/logs
   ```

4 Save the `webacc.cfg` file.

5 Skip to "Putting WebAccess Configuration Changes into Effect" on page 610.

Viewing WebAccess Application Log Files

For the default location of the WebAccess Application log files, see "Locating WebAccess Application Log Files" on page 621.

When logging is turned on, the WebAccess Application creates a new log file each day and each time it is restarted (as part of the web server startup). Therefore, you find multiple log files in the log file folder. The first four characters represent the date (*mmdd*). The next three characters identify the WebAccess Application (`waa`). A three-digit extension allows for multiple log files created on the same day. For example, a log file named `0518waa.001` indicates that it is a WebAccess Application log file, created on May 18.

For convenience, you can view WebAccess Application log files in the WebAccess Application console.

Interpreting WebAccess Application Log File Information

In its log file, the WebAccess Application records user activity in GroupWise WebAccess, along with a time stamp showing when the activity took place.

XVI Calendar Publishing Host

- Chapter 78, "Configuring the Calendar Publishing Host," on page 625
- Chapter 79, "Monitoring Calendar Publishing," on page 631
- Chapter 80, "Creating a Corporate Calendar Browse List," on page 633
- Chapter 81, "Managing Your Calendar Publishing Host," on page 635

For a complete list of port numbers used by the Calendar Publishing Host, see "Calendar Publishing Host Port Numbers" on page 730.

78 Configuring the Calendar Publishing Host

For Calendar Publishing (CalPub) Host system requirements, see "GroupWise Calendar Publishing Host System Requirements" in the *GroupWise 18 Installation Guide*. For detailed instructions about installing and setting up the GroupWise CalPub Host for the first time, see "Setting Up the GroupWise Calendar Publishing Host" in the *GroupWise 18 Installation Guide*.

The default configuration of the CalPub Host is adequate to begin publishing calendars. As your GroupWise system grows and evolves, you might need to modify its configuration to meet the changing needs of the users it services.

- "Using the CalPub Admin Console" on page 625
  - Changing Post Office Settings
  - Adjusting Log Settings
  - Configuring Authentication
  - Customizing the Calendar Publishing Host Logo
- "Using the calhost.cfg File" on page 627
  - Setting the Published Calendar Auto-Refresh Interval
  - Setting the Default Published Calendar View
  - Configuring an External POA IP Address
  - Providing an SSL Trusted Root Certificate

Using the CalPub Admin Console

Some aspects of the Calendar Publishing (CalPub) Host can be configured using the CalPub Admin console.

Logging In to the CalPub Admin Console

The CalPub Admin console is a browser-based administration tool that enables you to easily change the configuration of the CalPub Host.

1 Display the CalPub Admin console login page:

   `http://`*`network_address`*`/gwcal/admin`

2 Provide the administrator user and password for the CalPub Host Admin console, then click **Login**.

   For more information, see "Setting Up Calendar Publishing Administration" in the *GroupWise 18 Installation Guide*

Changing Post Office Settings

1 Log in to the CalPub Admin console.

The Post Office page provides the information that the CalPub Host needs in order to communicate with a POA to obtain calendar and free/busy information. The initial information was provided during installation. For more information, see "Configuring a POA for Calendar Publishing" in the *GroupWise 18 Installation Guide*.

2 Change the post office settings as needed.

   Post Office Network Address: Specify the IP address or DNS hostname of the POA that is configured for calendar publishing.

   Post Office TCP Port: Specify the calendar publishing port that the POA uses to communicate with the CalPub Host.

3 Click **Save** to save your changes.

Adjusting Log Settings

1 Log in to the CalPub Admin console, then click **Logging** to define log settings for the CalPub Host:

   Logging is enabled by default. Default settings are provided for the rest of the fields.

2 Change the CalPub Host log settings as needed:

   Enable Logging: Deselect this option to turn off CalPub Host logging.

   Log File Path: The default log file location varies by platform:

Linux:	`/var/opt/novell/groupwise/calhost/logs`
Windows:	`c:\novell\groupwise\calhost\logs`

   Change the log file settings as needed:

   Language: Select the language for the log files.

   Max Size for Log Files: Specify in kilobytes the maximum size for log files. When the combined size of log files reaches this size the oldest log files are deleted.

   Max Log File Age: Specify the number of days for the maximum age for a log file. When a log file reaches this age, it is deleted.

   Log Level: Select the level of detail that you want recorded in the log file.

   Use Tomcat Log File: Select this option if you want the same information logged to the Tomcat log file as is logged to the Calendar Publish Host log file. The location of the Tomcat log file varies by platform:

OES 11:	`/var/opt/novell/tomcat8/logs`
SLES 11:	`/usr/share/tomcat8/logs`
Windows:	`c:\novell\tomcat8\logs`

3 Click **Save** to save your changes.

Configuring Authentication

1 Log in to the CalPub Admin console, then click **Authentication**.

2 Change the authentication information as needed:

   Admin Service Address: Specify the IP address or DNS hostname of a GroupWise domain server. The default is the local host where the Calendar Publishing Host Application is running.

Admin Service Port Specify the Admin Service port number on the domain server.

3 Click **Save** to save your changes.

Customizing the Calendar Publishing Host Logo

1 Log in to the CalPub Admin console, then click **Customize** to modify the appearance of the Calendar Publishing web page.

2 Provided the information for your company logo:

Logo Image: Specify the full path and file name of the customized image file.

Logo Text: Specify the text to accompany the customized image.

Logo Text Position: Select **Top**, **Middle**, or **Bottom**, based on the example displayed in the box below the field.

3 Click **Save** to save your changes.

Putting the CalPub Host Configuration Changes into Effect

- "Accepting the Default Time Interval" on page 627
- "Immediately Putting the Configuration Changes into Effect" on page 627

Accepting the Default Time Interval

When you close the browser page, you are automatically logged out of the CalPub Host console.

The CalPub Host checks its configuration file (`calhost.cfg`) every 10 minutes. Therefore, it can take up to 10 minutes for the changes you made in the CalPub Admin console to take effect in the functionality of the CalPub Host.

Immediately Putting the Configuration Changes into Effect

You can also manually restart Tomcat in order to put the changes into effect immediately.

SLES 11:	`rcgrpwise-tomcat8 stop rcgrpwise-tomcat8 start`
Windows:	1. At the Windows server, click **Start** > **Administrative Tools** > **Services**. 2. Right-click **Tomcat 8**, then click **Restart**.

Using the calhost.cfg File

Some aspects of the CalPub Host cannot be configured in the CalPub Admin console, so you must manually edit the `calhost.cfg` file instead.

Editing the calhost.cfg File

The location of the `calhost.cfg` file varies by platform:

Linux:	`/var/opt/novell/groupwise/calhost`
Windows:	`c:\Micro Focus\GroupWise\calhost`

You can use any ASCII text edit that you prefer to edit the `calhost.cfg` file.

IMPORTANT: It is strongly recommended that you do not modify any settings that are not documented in the following sections.

Setting the Published Calendar Auto-Refresh Interval

By default, when users view a published calendar, the calendar view in the user's browser is not refreshed while users are viewing the calendar. You can configure the CalPub Host to automatically refresh the information that displays in a published calendar. This is especially helpful when calendars for resources such as conference rooms are published and displayed outside of the rooms.

1. Edit the `calhost.cfg` file.
2. Find the line that starts with:

   `Templates.Content.Refresh=`
3. Replace `0` (zero) with the number of seconds after which you want the CalPub Host to refresh the content of published calendars.
4. Save the `calhost.cfg` file, then exit the text editor.
5. Skip to "Putting the CalPub Host Configuration Changes into Effect" on page 627.

Setting the Default Published Calendar View

By default, published calendars are displayed in the Week view. A Day view and a Month view are also available.

1. Edit the `calhost.cfg` file.
2. Find the line that starts with:

   `User.Calendar.defaultView=`
3. Replace `Week` with `Day` or `Month` as desired.
4. Save the `calhost.cfg` file, then exit the text editor.
5. Skip to "Putting the CalPub Host Configuration Changes into Effect" on page 627.

Controlling Items Displayed

By default, published calendars display appointments, notes, and tasks. You can change what is displayed by following the steps below.

1. Edit the `calhost.cfg` file.
2. Find the following lines:

   `User.Calendar.Hide.appointment=false`

   `User.Calendar.Hide.note=false`

   `User.Calendar.Hide.task=false`
3. Change the ones you want to hide from `false` to `true`.
4. Save the `calhost.cfg` file, then exit the text editor.
5. Skip to "Putting the CalPub Host Configuration Changes into Effect" on page 627.

Configuring an External POA IP Address

If the POAs in your GroupWise system are configured to use an external IP address, you can configure the CalPub Host to always communicate with the POAs in your GroupWise system through that same external IP address. For more information about external POAs, see "Securing Client Access through an External Proxy Server" on page 150.

1 Edit the `calhost.cfg` file.

2 Find the line that starts with:

```
po.1.Is.IPAddress.External=
```

3 Replace `0` with `1` to enable this functionality.

4 Add the following lines to the `calhost.cfg` file to define the external POA:

```
po.1.IPAddress=ip_address
po.1.port=calendar_publishing_port
```

4a Replace *`ip_address`* with the external IP address used by the POAs in your GroupWise system.

4b Replace *`calendar_publishing_port`* with the calendar publishing port number for the POAs.

The default calendar publishing port number is 80.

5 Save the `calhost.cfg` file, then exit the text editor.

6 Skip to "Putting the CalPub Host Configuration Changes into Effect" on page 627.

Providing an SSL Trusted Root Certificate

If you are using an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory for authentication to your GroupWise system, and if you want to protect the CalPub Host console with an SSL connection, you must provide the trusted root certificate for the LDAP server.

1 Edit the `calhost.cfg` file.

2 Find the line that starts with:

```
Admin.Ldap.trustedRoot=
```

3 Specify the full path to the trusted root certificate file.

4 Save the `calhost.cfg` file, then exit the text editor.

5 Skip to "Putting the CalPub Host Configuration Changes into Effect" on page 627.

79 Monitoring Calendar Publishing

By monitoring the CalPub Host and the POAs that it communicates with, you can determine whether its current configuration is meeting the needs of your GroupWise users.

Viewing Calendar Publishing Status in the POA Console

1 Display the POA console at the following URL:

`http://network_address:port`

Replace *network_address* with the IP address or DNS hostname of a POA that is configured for calendar publishing and *port* is the POA HTTP port. The default HTTP port is 7181.

2 Click **Configuration**.

3 Under the **Internet Protocol Agent Settings** heading, view the configuration information about the POA's connection to the CalPub Host.

4 Click **Calendar Publishing Post Office List** to view all POAs in your GroupWise system that have been configured for calendar publishing.

5 On the Configuration page, click **Calendar Free/Busy Publishing User List** to view all users who have published free/busy information or personal calendars.

A list of all CalPub Hosts in your GroupWise system is also provided.

Using Calendar Publishing Host Log Files

The default log file location varies by platform:

Linux:	`/var/opt/novell/groupwise/calhost/logs`
Windows:	`c:\novell\groupwise\calhost\logs`

Logging is enabled by default. You can increase the amount of information that is logged. For more information, see "Adjusting Log Settings" on page 626.

Using POA Log Files

To find status information about how the CalPub Host is communicating with the POA, you can check the POA log files. For more information, see "Viewing and Searching POA Log Files" on page 167.

80 Creating a Corporate Calendar Browse List

The CalPub Host creates a browse list of published calendars. However, by default, no calendars are displayed in the calendar browse list. To create a corporate calendar browse list, you need to grant rights to specific users, or at the post office or domain level, in order to publish to the corporate calendar browse list.

In the GroupWise Admin console:

1. Browse to and click the name of an individual user.

   or

   Browse to and click the name of a post office or domain.
2. Click the **General** tab, then locate the **Calendar Publishing** section.
3. Select **Override**, then select **Enable Publishing of Calendars to the Browse List**.

   This grants the right to publish calendars to the calendar browse list.
4. Click **Save**, then click **Close** to return to the main Admin console window.

81 Managing Your Calendar Publishing Host

As circumstances change over time, you might need to change the configuration of your CalPub Host to better meet the needs of your GroupWise users.

Adding Multiple Calendar Publishing Hosts

Often, one CalPub Host is sufficient to service all Internet users who want to access your GroupWise users' calendar and free/busy information. However, you might want to add an additional CalPub Host for load balancing or to improve response time for Internet users in different geographical locations.

If you have users in remote locations, and response time is slow for these users, you can add a CalPub Host to a POA that is closer to these remote users.

NOTE: Sections referenced in the following steps are found in the *GroupWise 18 Installation Guide*.

---

1. Install the CalPub Host software to a remote web server.

   For instructions, see "Installing the GroupWise Calendar Publishing Host."
2. Add and configure the new CalPub Host.

   For instructions, see "Configuring the Calendar Publishing Host in the GroupWise Admin Console".
3. Restart the POAs for post offices that support calendar publishing so that the POAs pick up the configuration information for the new CalPub Host.
4. Restart Tomcat on the server where you installed the new CalPub Host to establish it as part of your GroupWise system.
5. Ensure that the new CalPub Host is accessible.

   For instructions, see "Testing GroupWise Calendar Publishing".
6. To improve performance when you set up multiple CalPub Hosts, follow the instructions in TID 7007208: "Load Balancing and High Availability for GroupWise Calendar Publishing" in the Micro Focus Support Knowledgebase (http://www.novell.com/support/).
7. Continue with "Assigning a Different Calendar Publishing Host to Users" on page 635.

Assigning a Different Calendar Publishing Host to Users

1. In the GroupWise Admin console, browse to and click the name of a user, or a post office with users to whom the new CalPub Host will be assigned.
2. Click **Client Options**.
3. Click the **Calendar** tab, then click **Web Calendar**.

4 In the **Web Calendar Publishing Host** field, select the new CalPub Host, then click the **Lock** button to ensure that the new CalPub Host setting overrides the previous setting.

5 Click **OK**.

6 Repeat Step 1 through Step 5 until you are finished moving users to each CalPub Host.

7 Notify the GroupWise users to whom the new CalPub Host as been assigned that they need to notify their Internet colleagues of the new URL for their published calendars and free/busy information.

Editing Calendar Publishing Host Configuration

Over time, you might need to set up the CalPub Host on a different web server with a different IP address or port number.

1 If necessary, install the CalPub Host to a new web server.

  For instructions, see "Installing the GroupWise Calendar Publishing Host" in the *GroupWise 18 Installation Guide*

2 In the GroupWise Admin console, click **System > Calendar Publishing**.

3 Click the name of the CalPub Host whose configuration you need to change.

  Do not change the URL unless absolutely necessary. Changing the URL would invalidate the URL that GroupWise users have sent to Internet colleagues to access published calendars and free/busy information.

4 Modify the IP address or port number of the web server as needed, then click **OK** twice.

5 Restart Tomcat where the modified CalPub Host is installed.

  For instructions, see "Immediately Putting the Configuration Changes into Effect" on page 627.

6 Restart the POA so that it picks up the updated configuration information for the modified CalPub Host.

7 Ensure that users can still access the CalPub Host.

  For instructions, see "Testing GroupWise Calendar Publishing" in the *GroupWise 18 Installation Guide*

Deleting a Calendar Publishing Host

1 If necessary, move users to a different CalPub Host.

  For instructions, see "Assigning a Different Calendar Publishing Host to Users" on page 635

2 In the GroupWise Admin console, click **System > Calendar Publishing**.

3 Select the CalPub Host to delete, then click **Delete**.

4 Click **OK**.

5 Restart Tomcat where the CalPub Host has been deleted.

  For instructions, see "Immediately Putting the Configuration Changes into Effect" on page 627.

6 Restart the POA that used to communicate with the deleted CalPub Host, so that the POA does not try to reestablish the connection.

XVI Monitor

For a complete list of port numbers used by Monitor, see “Monitor Agent Port Number” on page 730 and “Monitor Application Port Numbers” on page 730.

For detailed Linux-specific Monitor information, see Appendix C, “Linux Basics for GroupWise Administration,” on page 735.

82 Understanding the Monitor Agent Consoles

The Monitor Agent offers three different consoles where you can check the status of your GroupWise agents.

For a comparison of the capabilities of the three consoles, see Chapter 86, “Comparing the Monitor Consoles,” on page 673.

For detailed instructions about installing and starting the GroupWise Monitor Agent for the first time, see “Setting Up GroupWise Monitor” in the *GroupWise 18 Installation Guide*.

Windows Monitor Agent Server Console

The Monitor Agent server console is available for the Windows Monitor Agent but not for the Linux Monitor Agent.

All agent configuration tasks can be performed at the Monitor Agent server console, but some reports are not available.

Monitor Agent Console

The Monitor Agent console is platform-independent and can be viewed at the following URL:

`http://`*`web_server_address`*`:8200`

To create the Monitor Agent console display in your web browser, your web browser communicates directly with the Monitor Agent to obtain agent status information. You must be behind your firewall to use the Monitor Agent console. The Linux Monitor Agent does not have a server console.

The Monitor Agent console is divided into the Agent Groups window on the left and the Agent Status window on the right. You can use the Agents Groups window to create and manage agent groups in the same way that you can at the Windows Monitor Agent server console.

Several Monitor features are available at the Monitor Agent console that are not available at the Windows Monitor Agent server console or the Monitor web console. These are summarized in Chapter 86, “Comparing the Monitor Consoles,” on page 673.

Monitor Web Console

The Monitor web console is also platform-independent and can be viewed at the following URL:

`http://`*`web_server_address`*`/gwmon/gwmonitor`

To create the Monitor web console display, your web server communicates with the Monitor Application (a component of your web server), which then communicates with the Monitor Agent to obtain agent status information. This enables the Monitor web console to be available outside your firewall, while the Monitor Agent console can be used only inside your firewall.

The Monitor web console is divided into the Agent Groups window on the left and the Agent Status window on the right. Using the Agents Groups window, you can create and manage agent groups.

The Monitor web console does not include some features that are available at the Windows Monitor Agent server console and the Monitor Agent console. These are summarized in Chapter 86, "Comparing the Monitor Consoles," on page 673.

83 Configuring the Monitor Agent

For GroupWise Monitor system requirements, see "GroupWise Monitor System Requirements" in the *GroupWise 18 Installation Guide*. For detailed instructions about installing and starting the GroupWise Monitor Agent for the first time, see "Setting Up GroupWise WebAccess" in the *GroupWise 18 Installation Guide*.

The default configuration of the GroupWise Monitor Agent is adequate to begin monitoring existing GroupWise agents (Post Office Agents, Message Transfer Agents, and Internet Agents). You can also customize the configuration to meet your specific monitoring needs.

You configure the Monitor Agent at the Monitor Agent console:

`http://localhost:8200`

Selecting Agents to Monitor

By default, the Monitor Agent starts monitoring all GroupWise agents (Post Office Agents, Message Transfer Agents, and Internet Agents) in your GroupWise system, based on the information from a domain database (`wpdomain.db`). You might not want to continue monitoring all agents. Under certain circumstances, you might want to monitor agents that are not part of your local GroupWise system.

- "Filtering the Agent List" on page 641
- "Adding an Individual Agent" on page 642
- "Adding All Agents on a Server" on page 642
- "Adding All Agents on a Subnet" on page 642
- "Removing Added Agents" on page 642

Filtering the Agent List

You can configure the Monitor Agent to stop and start monitoring selected agents as needed.

1. In the Monitor Agent console, click **Preferences > Filter**.

   The **Filtered Out** list displays all agents that are not currently being monitored.
2. Select one or more agents in the Monitored list, then click **Remove** to move them to the **Filtered Out** list.
3. Click **OK**.

Agents in the **Filtered Out** list are not monitored and do not appear in the Monitor Agent console. To start monitoring a filtered-out agent, move it back to the **Monitored** list.

Adding an Individual Agent

You can start monitoring an individual agent anywhere in your GroupWise system or another GroupWise system.

1. In the Monitor Agent console, click **Preferences > Add Agents**.
2. Type the IP address of the server where the agent runs.
3. Type the port number the agent listens on.
4. Click **OK**.

   The agent is added to the list of monitored agents.

Adding All Agents on a Server

If you add a new server to your GroupWise system or want to monitor agents in a different GroupWise system, you can easily start monitoring all the agents running on that server.

1. In the Monitor Agent console, click **Preferences > Add Agents.**
2. Type the IP address of the new server, then click **OK**.

   All GroupWise agents on the new server are added to the list of monitored agents.

If the new server is part of your local GroupWise system, you can simply restart the Monitor Agent and it picks up all new agents in your system.

Adding All Agents on a Subnet

If you add several new servers to your GroupWise system or want to monitor agents in a different GroupWise system, you can easily start monitoring all the agents running on the same subnet.

1. In the Monitor Agent console, click **Preferences > Add Agents**.
2. Type the subnet portion of the IP addresses of the new servers, then click **OK**.

   All GroupWise agents on the subnet are added to the list of monitored agents.

If the new servers are part of your local GroupWise system, you can simply restart the Monitor Agent and it picks up all new agents in your system.

Removing Added Agents

To stop monitoring agents that you have manually added to the Monitor Agent’s configuration:

1. In the Monitor Agent console, click **Preferences > Remove Agents**.
2. Select the agents you want to remove, then click **Remove**.
3. Click **OK**.

Creating and Managing Agent Groups

You might find it convenient to group related agents together for monitoring purposes. Initially, all agents are in a single group with the same name as your GroupWise system.

Agent groups are displayed on the left side of the Monitor Agent console. When you select an agent group, the monitored agents in the group and their status information are listed on the right side of the Monitor Agent console.

You can create additional groups and subgroups as needed to make monitoring similar agents easier. You might want to create agent groups based on geographical areas, on administrative responsibilities, or on agent configuration similarities. The number of agents in the group is displayed to the right of the group name in the Agent Groups window.

In addition, by creating agent groups, you can provide configuration settings for monitoring just once for all agents in each group, rather than providing them individually for each agent in your GroupWise system.

NOTE: On Linux, you perform these tasks at the Monitor Agent console or Monitor console, using steps similar to those provided in this section.

Creating an Agent Group

In the Monitor Agent console:

1. In the Agent Groups window, click **Create**.
2. Type a name for the new group, select the parent group for the new group, then click **Create**.
3. In the Agent Status window, select one or more agents to add to the new group, then click **Move**.
4. In the list of available groups, select the new group, then click **Move**.
5. Click the new group to view its contents.

You can nest groups within groups as needed.

Managing Agent Groups

In the Monitor Agent console

- To rename an agent group, click **Rename**, type the new name, select the group to rename, then click **Rename**.
- To move an agent group, click **Move**, select the group to move, select the new location, then click **Move**.
- To delete an agent group, click **Delete**, select the group to delete, then click **Delete**.

Configuring an Agent Group

Configuration settings for monitoring can be set individually for each monitored agent, for each agent group, or for all monitored agents collectively.

You can establish default configuration settings for all agents by setting them on the root agent group that is named the same as your GroupWise system. By default, those default settings are inherited by each subgroup that you create thereafter. Groups, subgroups, and individual agents can be configured differently from the configuration provided at the higher level.

Configuring Monitoring Protocols

By default, the Monitor Agent uses HTTP to communicate with the agents it monitors. If HTTP is not available, the Monitor Agent changes automatically to SNMP.

Configuring the Monitor Agent for HTTP

You can customize how the Monitor Agent communicates with your web browser.

1. In the Monitor Agent console, click **Preferences > Setup**, then scroll down to the **HTTP Settings** section.
2. Modify the HTTP settings as needed:

   HTTP Refresh Rate: Specify the number of seconds after which the Monitor Agent sends updated information to the Monitor console. The default is 300 seconds (5 minutes).

   Poll Cycle: Specify the number of seconds after which the Monitor Agent polls all monitored GroupWise agents for updated information.

   By default, the Monitor Agent starts 20 threads to poll monitored agents. You can use the --pollthreads startup switch to adjust the number of threads. For more information, see Chapter 87, "Using Monitor Agent Startup Switches," on page 675.

   New Browser: Select this option to open a new web browser window whenever you display an agent console. This enables you to view the Monitor Agent console and an agent console at the same time, or to view two agent consoles at the same time for comparison.
3. Click **Submit** to put the new HTTP settings into effect.

Configuring the Monitor Agent for SNMP

You can customize how the Monitor Agent communicates with SNMP monitoring and management programs.

1. In the Monitor Agent console, click **Preferences > Setup**, then scroll down to the **SNMP Settings** section.
2. In the SNMP box, modify the SNMP settings as needed:

   SNMP Community Strings: Provide a comma-delimited list of community strings required to access the servers where GroupWise agents run.

   Time-out: Specify the number of seconds the Monitor Agent should wait for a response from servers where GroupWise agents run.

   Number of Retries: Specify how often the Monitor Agent should try to contact the servers where GroupWise agents run.

   Force polling through SNMP: Select this option to use SNMP polling instead of the default of XML polling when contacting servers where agents in the group run.
3. Click **Submit** to put the new SNMP settings into effect.
4. Ensure that the GroupWise agents you want to monitor using SNMP are enabled for SNMP.

   See "Setting Up SNMP Services for the POA" on page 168, "Setting Up SNMP Services for the MTA" on page 240, and "Setting Up SNMP Services for the GWIA" on page 314. The same instructions can be followed for all versions of the GroupWise agents.

Configuring Polling of Monitored Agents

By default, the Monitor Agent polls all monitored agents every five minutes. You can adjust the poll cycle as needed.

1 In the Monitor Agent console, select one or more agents, click **Preferences > Setup**, then scroll down to the **HTTP Settings** section.

2 Increase or decrease the poll cycle as needed, then click **Submit**.

Configuring Email Notification for Agent Problems

The Monitor Agent can notify you by email when agent problems arise.

- "Configuring Email Notification" on page 645
- "Customizing Notification Thresholds" on page 646

Configuring Email Notification

You can configure the Monitor Agent to notify one or more users by email if an agent goes down. You can also receive email confirmation messages showing that the Monitor Agent itself is still running normally.

1 In the Monitor Agent console, select one or more agents, then click **Preferences > Setup** to display the **Notify** settings.

2 Specify one or more comma delimited email and/or pager addresses to notify.

3 Specify the Internet domain name of your GroupWise system.

4 If the mail system to which email notification is being sent performs reverse DNS lookups, specify the IP address or hostname of a server to relay the notification messages through.

   The Monitor Agent should relay email notifications through a server that has a published DNS address.

5 Select the events to trigger email notification messages.

   - Agent Down
   - Server Down
   - Threshold Exceeded
   - State Returns to Normal

   If you want to be notified of more specific states, see "Customizing Notification Thresholds" on page 646.

6 Select the amount of time that you want to elapse before repeat email notifications are sent.

7 To monitor the Monitor Agent and assure it is functioning normally, specify the number of minutes between Monitor Agent email notification messages.

8 Click **Submit** to save the email notification settings.

Customizing Notification Thresholds

To refine the types of events that trigger email notification messages, you can create your own thresholds that describe very specific states. Using thresholds, you can configure the Monitor Agent to notify you of problem situations peculiar to your GroupWise system.

1 Ensure that notification has been properly set up.

For instructions, see “Configuring Email Notification” on page 645.

2 In the Monitor Agent console, click **Thresholds** on the Status page.

The tabs at the top of the window enable you to create a separate threshold for each type of GroupWise agent.

3 Select the type of agent to create a threshold for.

4 In the **Threshold Expression** field, select a MIB variable.

GroupWise agent MIB files are located in the `agents/mibs` folder. The MIB files list the meanings of the MIB variables and what type of values they represent. The meaning of the MIB variable selected in the **Threshold Expression** field is displayed above the field.

5 Select an operator from the drop-down list.

6 Type the value to test for.

For example, you might want to test the mtaOldestQMsg variable for a specific number of seconds that you consider to be too long for a message to be in the queue.

7 In the **State** field, select an existing state.

Icon	State
	Unknown
	Normal
	Informational
	Marginal
	Warning
	Minor
	Major
	Critical

or

Create a new state:

7a In the Monitor Agent console, click **Preferences > States**.

7b Type a name for the new state.

7c Select a severity level.

7d Provide instructions about how to handle the new state.

7e Click **Close** to save the new state.

8 Click **OK** to create the new threshold.

9 Repeat Step 2 through Step 8 for each type of agent that you want to create a customized state for.

10 Ensure that **Threshold Exceeded** is selected in the **Notification Events** box.

11 Click **OK** to save the new notification settings.

Configuring SNMP Trap Notification for Agent Problems

The Monitor Agent can throw SNMP traps for use by the Management and Monitoring component of Micro Focus ZENworks for Servers or any other SNMP management and monitoring program.

1 In the Monitor Agent console, select one or more agents, then click **Preferences** > **Setup** to display the **Notify** settings.

NOTE: The **Use Parent Notification Options** and **Apply Options to Subgroups** options are not available on Linux.

---

2 Select **Send SNMP Traps**, then click **OK**.

3 Ensure that the Monitor Agent is properly configured for SNMP.

For more information, see “Configuring the Monitor Agent for SNMP” on page 644.

Securing the Monitor Web Console

Accessing GroupWise agent status information from your web browser is very convenient. However, you might want to limit access to that information. You can configure the Monitor Agent to request a user name and password before allowing users to access the Monitor console. In addition, you can configure the Monitor Agent to detect break-in attempts in the form of repeated unsuccessful logins.

Use the --httpmonuser and --httpmonpassword startup switches when you start the Monitor Agent. For more information, see Chapter 87, “Using Monitor Agent Startup Switches,” on page 675.

Configuring Monitor Agent Log Settings

The Monitor Agent writes to two different types of log files:

- Event log files record error messages, status messages, and other types of event-related messages.
- History log files record dumps of all MIB values gathered during each poll cycle.

Log files can provide a wealth of information for resolving problems with Monitor Agent functioning or agent monitoring.

1 In the Monitor Agent console, click **Log > Log Settings**.

2 Fill in the fields:

Log File Path: Specify the full path of the folder where the Monitor Agent writes its log files.

The default log file location varies by platform.

Linux:	`/var/log/novell/groupwise/gwmon`
Windows:	`c:\ProgramData\Micro Focus\GroupWise Monitor`

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

Maximum Event Log File Age: Specify the number of days you want Monitor Agent event log files to remain on disk before being automatically deleted. The default event log file age is 30 days.

Maximum Event Log Disk Space: Specify the maximum amount of disk space for all Monitor event log files. When the specified disk space is used, the Monitor Agent overwrites existing Monitor Agent event log files, starting with the oldest. The default is 102400 KB (100 MB) of disk space for all Monitor Agent event log files.

Maximum History Log File Age: Specify the number of days you want Monitor Agent history log files to remain on disk before being automatically deleted. The default history log file age is 30 days.

Maximum History Log Disk Space: Specify the maximum amount of disk space for all Monitor history log files. When the specified disk space is used, the Monitor Agent overwrites existing Monitor Agent history log files, starting with the oldest. The default is 102400 KB (100 MB) of disk space for all Monitor Agent history log files.

3. Click **Submit** to put the new log settings into effect.
4. To view existing event logs, click **Log > Event Log**.
5. To view existing history log files, click **Log** > **History Log**.

Configuring Proxy Service Support for the Monitor Console

The main Monitor web console provides links to the agent consoles. Although you can access the Monitor console from outside your firewall, by default you cannot access the agent consoles from outside your firewall. To enable the Monitor web console to display the agent consoles from outside your firewall, you need to enable the Monitor Agent to support proxy service.

1. In a text editor, open the Monitor Application configuration file (`gwmonitor.cfg`).

   The location of the `gwmonitor.cfg` file varies by platform:

Linux:	`/var/opt/novell/groupwise/monitor`
Windows:	`c:\Micro Focus\GroupWise\monitor`

2. Locate the following line:

   ```
   Provider.GWMP.Agent.Http.level=basic
   ```

3. Change it to:

   ```
   Provider.GWMP.Agent.Http.level=full
   ```

The basic setting restricts use of the Monitor web console to within a firewall, while the full setting allows use of the console both inside and outside a firewall. A third setting, none, disables use of the console.

4. Save and exit the Monitor Application configuration file.
5. Start the Monitor Agent with the --proxy startup switch.

   For information about startup switches, see Chapter 87, "Using Monitor Agent Startup Switches," on page 675.

Without proxy service support enabled, the Monitor web console communicates directly with the GroupWise agent after it gets a GroupWise agent's address from the Monitor Agent. This process, however, does not work when communicating through a firewall.

With proxy service support enabled, all communication is routed through the Monitor Agent and Monitor Application (on the web server). As long as the web server can be accessed through the firewall, the Monitor web console can receive information about all GroupWise agents that the Monitor Agent knows about.

Supporting the GroupWise High Availability Service on Linux

The GroupWise High Availability Service, relies on the Monitor Agent to know when an agent has stopped and needs to be restarted. For more information, see "Automatically Restarting the Linux GroupWise Agents with the GroupWise High Availability Service" in the *GroupWise 18 Installation Guide*.

84 Configuring the Monitor Application

During installation, the GroupWise Monitor Application is set up with a default configuration. However, you can use the information in the following sections to optimize the Monitor Application configuration.

Editing the gwmonitor.cfg File

The location of the `gwmonitor.cfg` file varies by platform:

Linux:	`/var/opt/novell/groupwise/monitor`
Windows:	`c:\Micro Focus\GroupWise\monitor`

You can use any ASCII text edit that you prefer to edit the `gwmonitor.cfg` file.

IMPORTANT: We strongly recommended that you do not modify any settings that are not documented in the following sections.

Setting the Timeout Interval for Inactive Sessions

By default, administrators are logged out of the Monitor web console after 20 minutes if they have not performed any actions that generate requests. Actions such as polling agents for current status and running reports generate requests. Other actions, such as changing the view of existing information, and reading Help topics, do not generate requests.

The timeout interval provides security for GroupWise administrators who forget to log out of the Monitor web console. It also helps the performance of the web server by freeing the resources dedicated to that administrator's connection.

To adjust the timeout interval:

1. Open the `gwmonitor.cfg` file in a text editor.
2. Search to find the following line:

   ```
   Security.timeout=20
   ```

3. Change the default of `20` to the number of minutes that you prefer for the timeout interval.
4. Save the `gwmonitor.cfg` file.
5. Skip to "Putting the Monitor Configuration Changes into Effect" on page 654.

Adjusting Session Security

By default, the Monitor Application uses the web browser IP address of the Monitor user to confirm that, during the same session, it is always communicating with the same user. This is the highest form of security and works well for users on desktop workstations. However, for laptops and mobile devices that are carried to different places, possibly from one network segment to another, this level of security can cause interruptions in user sessions.

Other Monitor Application security features such as session cookies provide excellent security, even without the IP address checking. If you have multiple GroupWise administrators who check GroupWise status from various locations, you can turn off the need for confirming the web browser IP address to make the Monitor web consoles more stable for these mobile administrators.

To disable IP address checking:

1. Open the `gwmonitor.cfg` file in a text editor.
2. Search to find the following line:

   ```
   Security.UseClientIP.enable=
   ```

3. Change `true` to `false`.
4. Save the `gwmonitor.cfg` file.
5. Skip to "Putting the Monitor Configuration Changes into Effect" on page 654.

Accommodating Single Sign-On Products

Some organizations choose to place a single sign-on product such as NetIQ Access Manager (http://www.netiq.com/products/access-manager) between users on the web and the applications they access that are running behind the organization's firewall. If you use a single sign-on product with GroupWise Monitor, you must configure the Monitor Application to accommodate the single sign-on product.

1. Open the `gwmonitor.cfg` file in a text editor.
2. Search to find the following line:

   ```
   #Cookie.domain=.novell.com
   ```

3. Remove the pound sign (#) to activate the setting.
4. Replace `.novell.com` with the part of your organization's Internet domain name that is common between the single sign-on product and the web server where the Monitor Application is installed.

   For example, if the Access Manager server is at `nam.novell.com` and the Monitor Application is at `monitor.novell.com`, the domain name used to create cookies would be `.novell.com`, so that the cookies are accepted by both servers.
5. Save the `gwmonitor.cfg` file.
6. Skip to "Putting the Monitor Configuration Changes into Effect" on page 654.

Configuring Monitor Application Log Settings

Error messages and other information about Monitor Application functioning are written to log files. Log files can provide a wealth of information for resolving problems with Monitor Application functioning. Logging is enabled by default.

Locating Monitor Application Log Files

The default location of the Monitor Application log files varies by platform.

Linux:	`/var/opt/novell/groupwise/monitor/logs`
Windows:	`c:\Micro Focus\GroupWise\GWMonitor\logs`

You can change the location where the Monitor Application creates its log files. See Configuring Monitor Application Log Settings.

Configuring Monitor Application Log Settings

1. Open the `gwmonitor.cfg` file in a text editor.
2. Search to find the `Logging Information` section.
3. Adjust the following log settings as needed:

   Log.maxSize: Specify the maximum amount of disk space you want to use for Monitor Application log files. If the disk space limit is exceeded, the Monitor Application deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 102400 KB (100 MB).

   Log.maxAge: Specify the number of days you want to retain the log files. The Monitor Application retains log files for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 30 days.

   Log.level: There are three log levels:

   - **Normal (default)** Displays warnings and errors.
   - **Verbose:** Displays the Normal log level information, plus information messages and user requests.
   - **Diagnostic:** Displays all possible information. Use Diagnostic only if you are troubleshooting a problem with the Monitor Application.

     The Verbose and Diagnostic log levels do not degrade Monitor Application performance, but log files consume more disk space when Verbose or Diagnostic logging is in use.
4. Save the `gwmonitor.cfg` file.
5. Skip to "Putting the Monitor Configuration Changes into Effect" on page 654.

Viewing Monitor Application Log Files

For the default location of the Monitor log files, see "Viewing Monitor Application Log Files" on page 653.

When logging is turned on, the Monitor Application creates a new log file each day and each time it is restarted (as part of the web server startup). Therefore, you find multiple log files in the log file folder. The first four characters represent the date (*mmdd*). The next three characters identify the Monitor Application (`mon`). A three-digit extension allows for multiple log files created on the same day. For example, a log file named `0518mon.001` indicates that it is a Monitor Application log file, created on May 18.

Use your text editor of choice to view the Monitor Application log files.

Putting the Monitor Configuration Changes into Effect

Accepting the Default Time Interval

By default, the Monitor Application checks the `gwmonitor.cfg` file for changes every 10 minutes. When it finds changes, it puts the changes into effect without restarting Tomcat. If you are satisfied to have your changes put into effect within this time interval, no action is required on your part after you edit the `gwmonitor.cfg` file.

Changing the Default Time Interval

You can change the time interval at which the Monitor Application checks the `gwmonitor.cfg` file for changes.

1 Open the `gwmonitor.cfg` file in a text editor.

2 Search to find the following line:

```
Config.Update.check=10
```

3 Change `10` to the number of minutes Monitor Application to wait before checking for changes to its configuration file

4 Save the `gwmonitor.cfg` file.

Immediately Putting the Configuration Changes into Effect

You can also manually restart Tomcat in order to put the changes into effect immediately.

SLES 11:	`rcgrpwise-tomcat8 stop rcgrpwise-tomcat8 start`
Windows:	1. At the Windows server, click **Start** > **Administrative Tools** > **Services**. 2. Right-click **Tomcat 8**, then click **Restart**.

85 Using GroupWise Monitor

For a review of the three Monitor Agent consoles, see Chapter 82, "Understanding the Monitor Agent Consoles," on page 639. This section focuses on using the Monitor Agent console, although many of these tasks can also be performed at the Monitor web console.

Using the Monitor Agent Console

Initially, the Monitor Agent console lists all monitored GroupWise agents, along with their statuses.

After you create agent groups, the agents in each group are displayed when you select a group. For more information, see "Creating and Managing Agent Groups" on page 643.

You can display many types of monitoring information in the Monitor Agent console.

Viewing All Agents

After you have separated your agents into groups, you can still view all agents in your GroupWise system in a single list.

1 In the Monitor Agent console, click the root agent group, then click **Show Subgroup Agents**.

Viewing Problem Agents

In a single agent group or in a group with subgroups shown, you can filter the list to show only those agents whose status is not Normal.

1 In the Monitor Agent console, click **Problem**.

   Only problem agents are now displayed. If you leave the Monitor Agent with only problem agents displayed, many groups might appear empty because all agents have a status of **Normal**.

2 Click **Monitored**.

Viewing an Agent Console

An agent console can be displayed anywhere you have access to a web browser and the Internet.

1 In the Monitor Agent console, click the domain or post office link in the **Name** column.

For information about the agent consoles, see the GroupWise agent documentation:

- "Using the POA Console" on page 163
- "Using the MTA Console" on page 237
- "Using the GWIA Console" on page 311
- "Using the DVA Console" on page 373

Polling the Agents for Updated Status Information

By default, the Monitor Agent polls the monitored agents every five minutes. You can change the default poll cycle. For instructions, see "Configuring Polling of Monitored Agents" on page 645.

You can also manually poll monitored agents.

In the Monitor Agent console:

- To poll all agents, select all agents, then click **Poll**.
- To poll a specific agent, select the agent, then click **Poll**.
- To stop polling a specific agent, select the agent, then click **Suspend.** You can specify a time interval for the agent to be suspended, after which polling resumes automatically. By suspending polling, you prevent repeat notifications for a problem that is already being addressed.

  The suspended agent's status is listed as **Suspended**, accompanied by the same icon used for the Unknown status.
- To restart regular polling of an agent for which polling was suspended, select the agent, then click **Resume**.

Using the Monitor Web Console

The Monitor web console lists all GroupWise agents that the Monitor Agent is polling for status information. Use the following URL to access the Monitor console:

```
http://web_server_address/gwmon/gwmonitor
```

where *web_server_address* represents the IP address or hostname of the web server where the Monitor Application is installed.

Global features of the Monitor web console are available on icon buttons at the top of the main Monitor page.

Icon Button	Feature
	Problem
	Link Trace
	Link Configuration
	Global Options
	States
	Search

Click the **Problem** icon button to display only agents in your GroupWise system whose status is other than **Normal**. Click the name of your GroupWise system to display all agents again.

Click the status of an agent in the **Status** column to display agent status details.

Click an agent in the **Name** column to open its agent console. For information about the agent consoles, see "Viewing an Agent Console" on page 655.

Click an agent group in the left panel to display all monitored agents in the group. Click the **Problem** button above the agent list to display only those agents whose status is other than **Normal** in the agent group. The **Problem** button then changes to **Monitored**. Click the **Monitored** button to include working agents as well as problem agents in the list.

Click **Refresh** to update the agent status information. To modify the default poll cycle, see "Configuring Polling of Monitored Agents" on page 645.

To see what specific tasks can be performed at the Monitor console, see Chapter 86, "Comparing the Monitor Consoles," on page 673.

Generating Reports

You can generate reports on demand in the Monitor Agent console to help you manage message flow throughout your GroupWise system.

Link Trace Report

A link trace report enables you to follow the path a message would take between two GroupWise domains. A link trace report includes a list of all the domains through which a message would need to pass, along with their current status, link type, address, and number of messages currently queued in each domain. If any domain along the link path is closed, an error message is displayed.

If a message fails to arrive at its destination, this report can help you pinpoint its current location, so you can resolve the problem and get messages flowing smoothly again.

1. In the Monitor Agent console, click **Link Trace**.
2. Select a starting domain and a target domain.
3. If you want to trace the path back, which is the route status messages will take, select **Trace Return Path**.
4. Click **Trace.**

   If any domain in the path is closed, an error message displays so you know where the problem is occurring.

Link Configuration Report

A link configuration report enables you to list the links from one or more GroupWise domains to all other domains in your GroupWise system. This helps you identify inefficient link paths, loops, and unreachable domains. All domains must be open to obtain an accurate link map of your GroupWise system.

1. Ensure that all domains in your GroupWise system are open.

   You cannot obtain an accurate link map of your GroupWise system if any domains are closed.
2. In the Monitor Agent console, click **Link Configuration**.
3. Select **All Agents**

   or

   Select **Selected Agent** and select a specific agent from the drop-down list.

4 Click **Run**.

The list shows what domains a message would pass through to travel from the domain in the **Source** column to the domain in the **Destination** column. If a domain displays as closed, it means that the Monitor Agent could not contact the MTA for the domain or that a loop was detected in the link configuration.

Image Map Report

An image map enables you to create a visual picture of your GroupWise system, whether it resides in a single office building or spans the globe. You provide the maps; Monitor provides the up-to-the-minute status information at a glance.

- "Making Maps Available in Monitor" on page 658
- "Setting Up Maps" on page 658
- "Setting Up Regions" on page 659
- "Adding Agents to a Map" on page 661
- "Using an Image Map to Monitor Agents" on page 662

Making Maps Available in Monitor

1 Obtain useful maps from the Internet or another location.

You can use maps that vary in detail. For example, you could have one map the focuses on a particular corporate office building, another that shows offices throughout your country, and another that shows offices throughout the world. You can select from images in PNG and JPG format.

2 Copy the maps you want to use into the `maps` subfolder of the `monwork` folder.

The default location of the `monwork` folder varies by platform.

Linux:	`/tmp/gwmon/monwork/maps`
Windows:	`c:\ProgramData\Micro Focus\GroupWise Server\Monitor\monwork\maps`

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

You can change the location using the --monwork startup switch. For more information, see Chapter 87, "Using Monitor Agent Startup Switches," on page 675

3 Continue with Setting Up Maps.

Setting Up Maps

1 In the Monitor Agent console, click **Map**.

Initially, no maps are available in Monitor.

2 Click **New** to display all the maps that are available in the `maps` folder.

The file name of each map is displayed below it.

3 Click the map that you want to set up, specify a custom name for the map, then click **Create**.

This makes the map available for use in Monitor.

4 To set up additional maps for use in Monitor, click **Done** to return to the Image Map Selection menu, then repeat Step 2 and Step 3 for each map that is available in the `maps` folder to make it available in Monitor.

5 If you want to make one or more smaller-scale maps available from a large-scale map, continue with "Setting Up Regions" on page 659.

or

If your maps are all independent from each other, skip to "Adding Agents to a Map" on page 661.

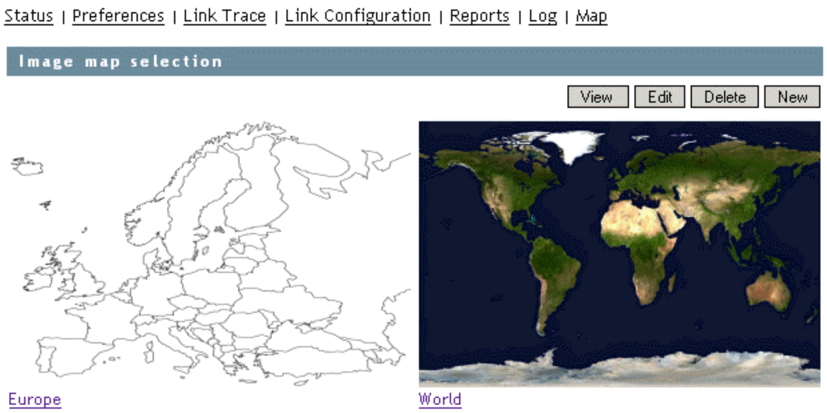
Setting Up Regions

If some of your maps are subsets of other maps, you can set up a large-scale map so that it links to one or more smaller-scale maps. For example, a map of the world could have a region for each continent or country, or a map of a city or country could have a region for each office where GroupWise domains or post offices are located.

1 Set up at least two maps in Monitor.

For instructions, see "Making Maps Available in Monitor" on page 658.

2 In the Monitor Agent console, click **Map** to display the maps that are available in Monitor.



The custom name of each map is displayed below it.

3 Click **Edit**, then click a large-scale map.

4 In the drop-down list, scroll down through the agents, click the smaller-scale map that you want to define as a region, then click on the large-scale map to refresh the view.

5 Click points on the map to surround the region.

6 Click **Done** to define the region.

With a very wide map, you need to scroll horizontally to display the **Done** button.

The region appears labeled on the large-scale map.

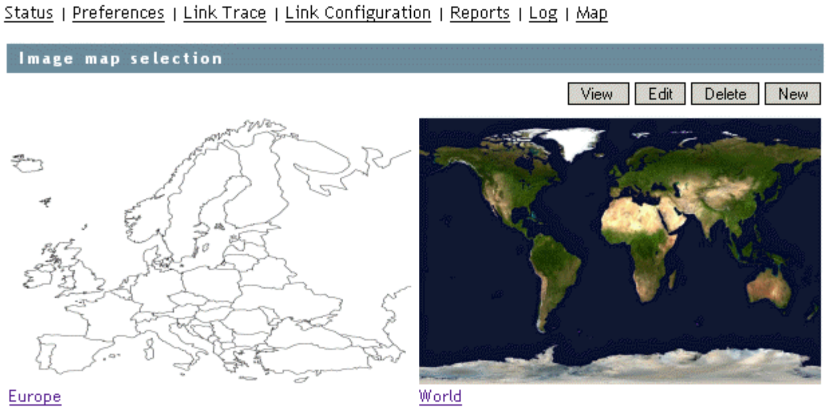
7 To define more regions on the large-scale map, click **Done** to return to the available maps, then repeat Step 3 through Step 6 for each region.

or

To place agents on a map, continue with Adding Agents to a Map.

Adding Agents to a Map

1 In the Monitor Agent console, click **Map** to display the maps that are available in Monitor.



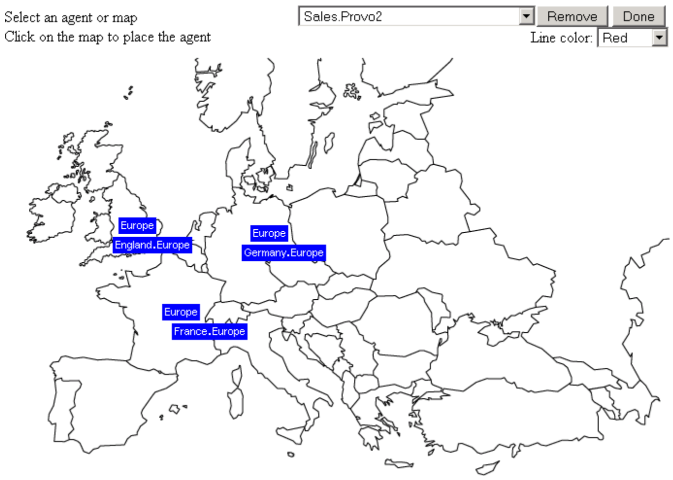
The custom name of each map is displayed below it.

2 Click **Edit**, then click the map where you want to add agents.

3 Select an agent in the drop-down list, then click the place on the map where that agent is located.

The agent name appears in a blue box.

4 Select additional agents and locations as needed.



5 In the **Line Color** drop-down list, select the color to use to show links between locations.

Ensure that you select a color that shows up well on the particular map. Lines display on the map only when links between locations are down.

6 Click **Done** when the map includes all the needed GroupWise agents in their respective locations.

7 Continue with Using an Image Map to Monitor Agents.

Using an Image Map to Monitor Agents

1 In the Monitor Agent console, click **Map > View**.

2 Click a map to view agent status.

or

If the map has regions, click a region to display the map that has agent status for that region.

At this point, the Monitor Agent checks the status of each agent on the map. Any agent that is down or that has a status of **Major**, **Critical**, or **Warning** displays in red on the map. Agents with a lower status do not display on the map. If a link between agents is down, a line displays between the agents.

Environment Report

An environment report lists all monitored agents, along with each agent's location, version, IP address, port number, and operating system information.

In the Monitor Agent console:

1 Click **Reports > Environment**.

User Traffic Report

A user traffic report enables you to determine how many messages a user has sent outside his or her post office. The user traffic report lists all messages sent by a specified user during a specified date/ time range, along with date, time, and size information for each message. You can also generate a user traffic report for all users whose messages pass through a selected domain.

In order for the information to be available to generate a user traffic report, you must configure the MTA to perform message logging. See "Enabling MTA Message Logging" on page 228.

In the Monitor Agent console:

1 Click **Reports > User Traffic**.

2 Select the user's domain or the domain you want to generate a user traffic report for.

3 Type the GroupWise user name that you want to create a report for.

or

Leave the field blank to create a report for all users whose messages pass through the selected domain.

4 Click **Run**.

Link Traffic Report

A link traffic report enables you to determine how many messages are passing from a selected GroupWise domain across a specified link. The link traffic report lists the total number and total size of all messages passing through the link during each hour or half hour of operation.

In order for the information to be available to generate a link traffic report, you must configure the MTA to perform message logging. See "Enabling MTA Message Logging" on page 228.

In the Monitor Agent console:

1 Click **Reports** > **Link Traffic**.

2 Select the source domain of the link, then click **Next**.

   The list includes all domains that the Monitor Agent uses XML to communicate with. If the Monitor Agent must use SNMP to communicate with a domain, that domain is not included in the list.

3 Select the other end of the link, which could be another domain, a post office, or a GWIA.

4 Click **Run**.

Message Tracking Report

A message tracking report enables you to track an individual message through your GroupWise system. The message tracking report provides information about when a message was sent, what queues the message has passed through, and how long it spent in each message queue. If the message has not been delivered, the message tracking report shows where it is.

In order for the information to be available to generate a message tracking report, you must configure the MTAs in your GroupWise system to perform message logging. See "Enabling MTA Message Logging" on page 228.

In addition, you need to determine the message ID of the message. Have the sender check the Sent Item Advanced Properties of the message in the GroupWise client. The **Message Id** field displays the message ID of the message; for example, 3AD5EDEB.31D : 3 : 12763.

In the Monitor Agent console:

1 Click **Reports** > **Message Tracking**.

2 Select the domain where you want to start tracking.

3 Type the message ID of the message to track.

   You can obtain the message file ID in the GroupWise client. Open the Sent Items folder, right-click the message, click **Properties**, then click the **Style** drop-down list and click **Advanced Properties**. The **Message Id** field displays the message file ID; for example, 3A75BAB9.FF1 : 8 : 31642.

4 Click **Track**.

Performance Testing Report

A performance testing report enables you to measure how long it takes messages to travel through your GroupWise system. The performance testing report lists each domain that a performance test message was sent to, when it was sent by the Monitor Agent, and the number of seconds between when it was sent and when the Monitor Agent received a response from the tested agent.

In order run a performance testing report, you must configure the Monitor Agent for performance testing. See "Measuring Agent Performance" on page 665.

Connected User Report

The Connected Users report lists all users that are currently connected to POAs throughout your GroupWise system. It lists user name; client version, date, and platform; login time; and the IP address of the client user.

In the Monitor Agent console:

1 Click **Reports** > **Connected Users**.

Gateway Accounting Report

The Gateway Accounting report shows traffic through a GWIA. For example, you can use a Gateway Accounting report to track traffic to and from the Internet through a particular GWIA.

In order to run a Gateway Accounting report, you must configure the Monitor Agent to collect gateway accounting data. See "Collecting Gateway Accounting Data" on page 667.

Trends Report

The Trends report presents graphs of agent MIB variables as sampled over time. Graphs are generated based on data gathered from Monitor Agent log files. The quality of the graphs depends on the quantity of data that has been gathered when the graph is generated.

In the Monitor Agent console:

1 Click **Reports** > **Trends**.
2 Click the type of agent for which you want to set up a Trends report.
3 Specify a unique name for the Trend report.
4 Select the MIB variables that you want to collect values for over time, then click **Add Trend**.
   The Trend report appears in the **Agent Trends** list.
5 Click the Trend report to view the graphs.

Down Time Report

The Down Time report graphically illustrates how much time each GroupWise agent has been down during the day.

In the Monitor Agent console:

1 Click **Reports** > **Down Time**.

Measuring Agent Performance

To test the performance of the agents in your GroupWise system, you can send performance test messages from a specially configured Monitor domain to target domains anywhere in your GroupWise system. The Monitor Agent measures the amount of time it takes for replies to return from the target domains, which lets you ascertain the speed at which messages flow through your GroupWise system.

Setting Up an External Monitor Domain for Agent Performance

Before you can use the GroupWise Performance Testing feature to configure and enable GroupWise performance testing, you must create a specially configured Monitor domain and select an MTA to receive performance test messages from the Monitor Agent. It does not matter which MTA you decide to use. It could be the MTA for the domain to which the external Monitor domain is linked.

The Monitor Agent uses an external GroupWise domain as part of measuring GroupWise agent performance. By creating an external domain, you enable the Monitor Agent to approximate the round-trip time for email messages to travel to recipients and for status messages to travel back to senders. If you also plan to set up gateway accounting reports, you can use this same external domain for collecting accounting data. For more information, see "Collecting Gateway Accounting Data" on page 667.

1. In the GroupWise Admin console, connect to a domain where the MTA will communicate with the Monitor Agent for the purpose of measuring agent performance.
2. Create an external GroupWise domain.

   For background information about external GroupWise domains, see "Using an External Domain to Connect GroupWise Systems" on page 112.
3. Name the external domain to reflect its role in your GroupWise system.

   For example, you could name it ExternalMonitorDomain.
4. Continue with Configuring the Link for the External Monitor Domain.

Configuring the Link for the External Monitor Domain

The Monitor Agent needs to send its performance testing messages to a specific MTA in your GroupWise system. It does not matter which MTA you decide to use. It could be the MTA for the domain to which the external Monitor domain is linked.

1. In the GroupWise Admin console, click **System > Link Configuration** to open the Link Configuration tool.
2. In the **Source** column, select the domain whose MTA you want the Monitor Agent to communicate with.
3. In the **Destination** column, select the external domain that you just created.
4. Configure the outbound link from the selected MTA to the external Monitor domain.

   4a Specify the IP address of the server where the Monitor Agent runs.

   4b Specify a unique port number for the MTA to use to communicate with the Monitor Agent.

   4c Click **Save**, then click **Close** to exit the Link Configuration tool.
5. Continue with Configuring the Monitor Agent for Agent Performance Testing.

Configuring the Monitor Agent for Agent Performance Testing

After you have created an external Monitor domain and configured a link from it to an MTA, you are ready to configure the Monitor Agent for performance testing.

1. In the Monitor Agent console, click **Preferences > Setup**, then scroll down to the **Performance Testing** section.
2. Fill in the fields:

   Domain to Send Messages To: Select the external Monitor domain that you configured for system performance testing.

   You might need to restart the Monitor Agent in order to see the new Monitor domain in the drop-down list.

   Minutes between Messages: Specify in minutes the time interval for the Monitor Agent to send performance test messages.

   Enable GroupWise Performance Testing: Select this option to turn on performance testing. Deselect this option when you have finished your performance testing.

   Send Performance Messages To: Select **All Agents** to send performance test messages to all domains in your GroupWise system. Select **Monitored Agents** to send performance test messages only to the agents currently listed at the Monitor Agent console.
3. Click **Submit** to put the performance testing settings into effect.
4. Continue with "Viewing Agent Performance Data" on page 666.

Viewing Agent Performance Data

The information gathered by the Monitor Agent through performance test messages is recorded in the Monitor history log.

In the Monitor Agent console:

1. Click **Log** > **History Log**.
2. Select a history log file, then click **View**.
3. Continue with Viewing an Agent Performance Report.

Viewing an Agent Performance Report

A performance testing report enables you to measure how long it takes messages to travel through your GroupWise system. The performance testing report lists each domain that a performance test message was sent to, when it was sent by the Monitor Agent, and the number of seconds between when it was sent and when the Monitor Agent received a response from the tested agent.

In the Monitor Agent console:

1. Click **Reports** > **Performance Testing**.
2. Select **All Domains** to generate a performance testing report for all domains in your GroupWise system.

   or

   Select one domain to generate a performance testing report for it.

3 Click **Run** to generate the performance testing report.

4 Continue with Receiving Notification of Agent Performance Problems.

Receiving Notification of Agent Performance Problems

If you want the Monitor Agent to notify you if system performance drops to an unacceptable level, you can create a threshold to check the `mtaLastResponseTime` and `mtaAvgResponseTime` MIB variables. The average response time is a daily average that is reset at midnight. See "Customizing Notification Thresholds" on page 646 for setup instructions.

Collecting Gateway Accounting Data

In order to run a Gateway Accounting report in Monitor, you must configure your GroupWise system to collect accounting files. The GWIA can be configured to generate accounting files. For more information, see "Tracking Internet Traffic with Accounting Data" on page 290. Then, the accounting files are collected and sent to the Monitor Agent for processing to create the Gateway Accounting report.

- "Setting Up an External Monitor Domain for Gateway Accounting" on page 667
- "Configuring the Link for the External Monitor Domain" on page 668
- "Configuring the Monitor Agent to Communicate through the External Monitor Domain" on page 668
- "Setting Up an External Post Office and External User for the Monitor Agent" on page 668
- "Receiving and Forwarding the Accounting Files" on page 669
- "Viewing the Gateway Accounting Report" on page 670

Setting Up an External Monitor Domain for Gateway Accounting

In order to collect accounting data, you must create a specially configured Monitor domain and select an MTA to send accounting files through it to the Monitor Agent. The Monitor Agent needs the external domain to house an external post office where there is an external user that receives the accounting files from the GWIA.

1 (Conditional) If you are already using the GroupWise Performance Testing feature, use the same external domain and MTA for gathering accounting data.

   Skip to "Setting Up an External Post Office and External User for the Monitor Agent" on page 668.

   For more information, see "Measuring Agent Performance" on page 665.

2 In the GroupWise Admin console, connect to a domain where the MTA will communicate with the Monitor Agent for the purpose of gathering accounting data.

3 Create an external GroupWise domain.

   For background information about external GroupWise domains, see "Using an External Domain to Connect GroupWise Systems" on page 112.

4 Name the external domain to reflect its role in your GroupWise system.

   For example, you could name it ExternalMonitorDomain.

5 Continue with Configuring the Link for the External Monitor Domain.

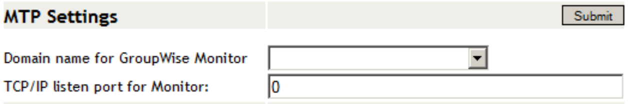
Configuring the Link for the External Monitor Domain

The Monitor Agent needs to receive accounting data from a specific MTA in your GroupWise system. It can be the MTA for the domain to which the external Monitor domain is linked.

1. In the GroupWise Admin console, click **System > Link Configuration** to open the Link Configuration tool.
2. In the **Source** column, select the domain whose MTA you want the Monitor Agent to communicate with.
3. In the **Destination** column, select the external domain that you just created.
4. Configure the outbound link from the selected MTA to the external Monitor domain.
   - **4a** Specify the IP address of the server where the Monitor Agent runs.
   - **4b** Specify a unique port number for the MTA to use to communicate with the Monitor Agent.
   - **4c** Click **Save**, then click **Close** to exit the Link Configuration tool.
5. Continue with Configuring the Monitor Agent to Communicate through the External Monitor Domain.

Configuring the Monitor Agent to Communicate through the External Monitor Domain

1. In the Monitor Agent console, click **Preferences**, then scroll down to the **MTP Settings** section.



2. Select the external Monitor domain in the drop-down list.
3. Specify the same port number that you specified in Step 4b in “Configuring the Link for the External Monitor Domain” on page 668.
4. Click **Submit**.
5. In the MTA console for the MTA in the domain that the external Monitor domain links to, verify that the link to the external Monitor domain is open.
6. Continue with Setting Up an External Post Office and External User for the Monitor Agent.

Setting Up an External Post Office and External User for the Monitor Agent

Now that you have set up the link for the accounting data to flow through, you need to create an external user to receive the accounting files.

1. Create an external post office:
   - **1a** In the GroupWise Admin console, click **Post Offices**, then click **New > External Post Office**.
   - **1b** Name the external post office to reflect its role, such as ExternalMonitorPO.
   - **1c** Select the external domain that you created in “Setting Up an External Monitor Domain for Gateway Accounting” on page 667.
   - **1d** Click **OK**.

2 Create an external user:

2a In the GroupWise Admin console, browse to and click the name of the external post office, then click **New** to add a new external user.

2b Name the external user to reflect its role, such as ExternalMonitorUser.

2c Click **OK**.

3 Designate a user as a gateway accountant to receive the accounting files:

As messages flow through a gateway such as the GWIA, the gateway logs the traffic and sends the accounting records to the gateway accountant once each day. For background information, see “Tracking Internet Traffic with Accounting Data” on page 290.

3a (Conditional) If you already have an accountant designated for each GWIA where you want to run accounting reports, skip to “Receiving and Forwarding the Accounting Files” on page 669.

3b Browse to and click a GWIA to process the accounting files.

3c On the **GroupWise** tab, click **Administrators**.

3d Select the user in the list of administrators, then click **Accountant**.

4 Continue with Receiving and Forwarding the Accounting Files.

5 Click **Save**, then click **Close** to return to the main Admin console window.

Receiving and Forwarding the Accounting Files

Each GWIA sends the accounting files to the accountant. The accountant then must forward the accounting files to the external Monitor user that you set up in “Setting Up an External Post Office and External User for the Monitor Agent” on page 668.

1 In the GroupWise client, create a new rule to forward all accounting messages to the external Monitor user in the external Monitor post office.

A typical subject line for an accounting message is Agent Accounting Data File.

2 In order to establish the link for the first time, restart the Monitor Agent and the MTA for the domain that the external Monitor domain is linked to.

3 Verify that the accounting files are being received by the Monitor Agent:

3a In the Monitor Agent console, click **Log > Gateway Accounting Logs**.

3b Select the GWIA, then click **View Accounting Logs**.

If files are listed, then accounting data is successfully arriving to the Monitor Agent. The Monitor Agent uses the accounting log files to generate Gateway Accounting reports.

The accounting log files on stored on the server where the Monitor Agent is running. The default location varies by platform.

Linux:	`/var/log/novell/groupwise/gwmon/acct`
Windows:	`c:\ProgramData\Micro Focus\GroupWise\Monitor\acct`

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

4 Continue with Viewing the Gateway Accounting Report.

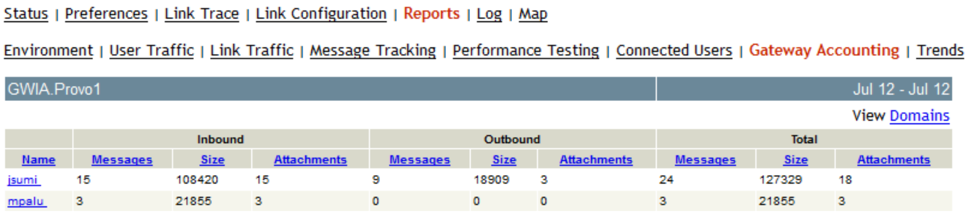
Viewing the Gateway Accounting Report

After accounting files are being successfully sent to the Monitor Agent for processing, you can view the Gateway Accounting report in your web browser.

1 In the Monitor Agent console, click **Reports > Gateway Accounting**.

2 Select the GWIA for which you want to view accounting reports, then click **View Accounting Reports**.

   The initial report lists all users who have sent and received messages through the GWIA. It lists the number of messages, the size of the messages, and the number of attachments. You can sort the list by any column heading.



3 In the **Users** list, click a user to list all messages sent to and from the user.

4 In the list of messages, click a message ID to run a Message Tracking report for that message.

   For more information, see "Message Tracking Report" on page 663.

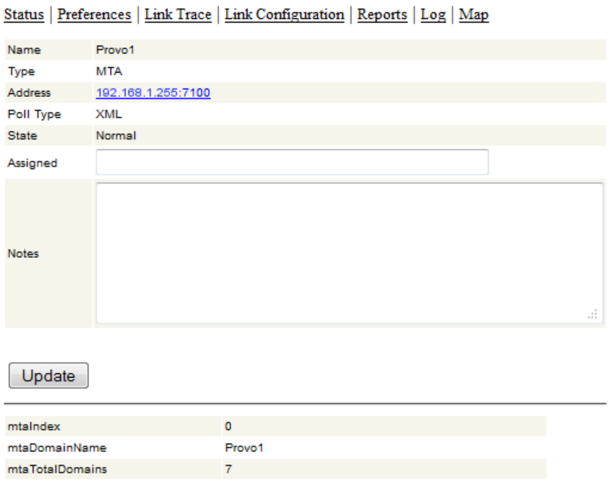
5 In the **Users** list, click **View Domains** to list the Internet domains associated with the GWIA.

6 In the list of domains, click an Internet domain to list all messages sent and received through that Internet domain.

Assigning Responsibility for Specific Agents

If multiple GroupWise administrators manage the agents throughout your GroupWise system, you can assign a contact for each agent. Or, in a help desk environment, a person can be assigned to an agent when a problem occurs. The person assigned to the agent can record notes about the functioning of the agent, which are then available to other administrators.

1 In the Monitor Agent console, click the agent status link in the **Status** column.



2 In the **Assigned** field, type the name of the GroupWise administrator who is responsible for this agent.

The name is displayed to the right of the agent status in the status window of the Monitor Agent console and the Monitor web console.

3 In the **Notes** field, type any comments you might have about the agent.

If a problem with the agent occurs, the **Thresholds** field and the **Suggestions** field display helpful information about the problem if you have set up customized thresholds.

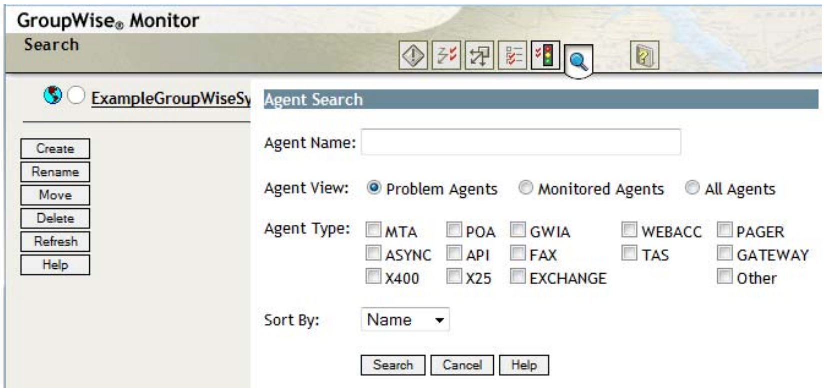
For more information, see "Customizing Notification Thresholds" on page 646.

4 Click **Update** to save the information about who is assigned to the agent.

Searching for Agents

If you monitor a large number of agents, the list displayed in the Monitor console can become very long. You can easily search for an individual agent or for a group of related agents.

1 In the Monitor web console, click the **Search** icon.



2 Type the name of an agent.

or

Select **Problem Agents** to list all agents whose status is other than **Normal**.

or

Select one or more types of agent to list.

3 Select how you want the list of agents sorted (by name, type, or version).

4 Click **Search**.

The results display on the Search page with the same functionality as is available on the main Monitor web console page.

86 Comparing the Monitor Consoles

Many aspects of agent monitoring are available in one or more of the Monitor consoles. The table below summarizes agent monitoring features and where they are available.

Task	Monitor Agent Console	Monitor Web Console	Windows Monitor Agent Server Console
Selecting Agents to Monitor	Yes	No	Yes
Creating and Managing Agent Groups	Yes	Yes	Yes
Viewing All Agents	Yes	Yes if not in groups	Yes
Viewing Problem Agents	Yes	Yes	Yes
Viewing an Agent Console	Yes	Yes	Yes
Searching for Agents	No	Yes	No
Assigning Responsibility for Specific Agents	Yes	Yes	Yes
Configuring the Monitor Agent for HTTP	Yes	Yes	Yes
Configuring the Monitor Agent for SNMP	Yes	Yes	Yes
Configuring Polling of Monitored Agents	Yes	Yes	Yes
Configuring Email Notification for Agent Problems	Yes	Yes	Yes
Configuring SNMP Trap Notification for Agent Problems	Yes	Yes	Yes
Securing the Monitor Web Console	Authentication: Yes Intruder Lockout: No	No	Yes
Configuring Monitor Agent Log Settings	Yes	Yes	Yes
Generating Reports	Yes	Yes	Yes
Link Trace Report	Yes	Yes	Yes
Link Configuration Report	Yes	Yes	Yes
Image Map Report	Yes	No	No
Environment Report	Yes	No	Yes
User Traffic Report	Yes	No	Yes
Link Traffic Report	Yes	No	Yes
Message Tracking Report	Yes	No	Yes
Performance Testing Report	Yes	No	Yes
Connected User Report	Yes	No	No
Gateway Accounting Report	Yes	No	No

Trends Report	Yes	No	No
Down Time Report	Yes	No	No

87 Using Monitor Agent Startup Switches

GroupWise Monitor Agent startup switches must be used on the command line when you start the Monitor Agent, or in a script or batch file created to start the Monitor Agent. The Monitor Agent does not have a startup file for switches.

Linux: If you start the Monitor Agent by running the `gwmon` executable, you can create a script like the following:

```
/opt/novell/groupwise/agents/bin/gwmon --home /domain_folder
                                       --other_switches &
```

If you start the Monitor Agent by running the `grpwise-ma` script, you can edit the MA_OPTIONS variable to include any switches you want to set.

Windows: If you are running the Monitor Agent as an application, you can create a batch file like the following:

```
c:\Program Files\Micro Focus\GroupWise Server\Monitor\gwmon.exe
                                     /startup_switch /startup_switch ...
```

You can create a desktop icon for your batch file, or you can add startup switches to the Monitor Agent desktop icon that is created when you install the Monitor Agent.

If you are running the Monitor Agent as a Windows service, you can provide startup options in the **Start Parameters** field on the **General** tab of the Monitor Agent service **Properties** dialog box.

The table below summarizes Monitor Agent startup switches for all platforms and how they correspond to configuration settings in the Windows Monitor Agent Server Console.

Switch starts with: a b c d e f g h i j k l m n o p q r s t u v w x y z

Linux Monitor Agent	Windows Monitor Agent	Windows Monitor Agent Server Console
--hapassword	/hapassword	N/A
--hapoll	/hapoll	N/A
--hauser	/hauser	N/A
--help	/help	N/A
--home	/home	N/A
--httpagentpassword	/httpagentpassword	**Configuration > Poll Settings > HTTP Password**
--httpagentuser	/httpagentuser	**Configuration > Poll Settings HTTP User**
--httpcertfile	/httpcertfile	N/A
--httpmonpassword	/httpmonpassword	**Configuration > HTTP > HTTP Password**
--httpmonuser	/httpmonuser	**Configuration > HTTP > HTTP User**
--httpport	/httpport	**Configuration > HTTP > HTTP Port**
--httpssl	/httpssl	N/A

Linux Monitor Agent	Windows Monitor Agent	Windows Monitor Agent Server Console
--ipa	/ipa	N/A
--ipp	/ipp	N/A
--lang	/lang	N/A
--log	/log	**Log > Log Settings > Log File Path**
--monwork	/monwork	N/A
--nosnmp	/nosnmp	N/A
--pollthreads	/pollthreads	N/A
--proxy	/proxy	N/A
--tcpwaitconnect	/tcpwaitconnect	N/A

NOTE: The Monitor Agent console does not include any settings comparable to the Monitor Agent startup switches.

--hapassword

Specifies the password for the Linux user name that the Monitor Agent uses to log in to the Linux server where the GroupWise High Availability service is running. See "Supporting the GroupWise High Availability Service on Linux" on page 649.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--hapassword *password*	/hapassword-*password*
Example:	--hapassword high	/hapassword-high

See also --hauser and --hapoll.

--hapoll

Specifies in seconds the poll cycle on which the Monitor Agent contacts the GroupWise High Availability service to provide agent status information. The default is 120. The actual duration of the poll cycle can vary from the specified number of seconds because the actual duration includes the time during which the Monitor Agent is checking agent status and restarting agents as needed. Then the specified poll cycle begins again and continues for the specified number of seconds. See "Supporting the GroupWise High Availability Service on Linux" on page 649.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--hapoll *seconds*	/hapoll-*seconds*
Example:	--hapoll 240	/hapoll-60

See also --hauser and --hapassword.

--hauser

Specifies the Linux user name that the Monitor Agent can use to log in to the Linux server where the GroupWise High Availability service is running. See "Supporting the GroupWise High Availability Service on Linux" on page 649.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--hauser *user_name*	/hauser-*user_name*
Example:	--hauser gwha	/hauser-gwha

See also --hapassword and --hapoll.

--help

Displays the Monitor Agent startup switch Help information. When this switch is used, the Monitor Agent does not start.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--help	/help

--home

Specifies a domain folder where the Monitor Agent can access a domain database (`wpdomain.db`). From the domain database, the Monitor Agent can determine which agents to monitor, what user names and passwords are necessary to access them, and so on.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--home /*folder*	/home-[*svr*\][*vol*:]*dir* /home-*svr**vol**dir* /home-[*drive*:]*dir* /home-*svr**sharename**dir*
Example:	--home /gwsystem/provo2	/home-\provo2 /home-mail:\provo2 /home-server2\mail:\provo2 /home-\\server2\mail\provo2 /home-\provo2 /home-m:\provo2 /home-\\server2\c\mail\provo

See also --ipa and --ipp.

--httpagentpassword

Specifies the password for the Monitor Agent to prompt for when contacting monitored agents for status information. Providing a password is optional. See “Configuring the Monitor Agent for HTTP” on page 644.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpagentpassword *unique_password*	/httpagentpassword-*unique_password*
Example:	--httpagentpassword WatchIt	/httpagentpassword-WatchIt

See also --httpagentuser.

--httpagentuser

Specifies the user name for the Monitor Agent to use when contacting monitored agents for status information. Providing a user name is optional. See “Configuring the Monitor Agent for HTTP” on page 644.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpagentuser *unique_user_name*	/httpagentuser-*unique_user_name*
Example:	--httpagentuser AgentWatcher	/httpagentuser-AgentWatcher

See also --httpagentpassword.

--httpcertfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the Monitor Agent and the Monitor console displayed in your web browser. See “Securing the Monitor Web Console” on page 647.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpcertfile /*dir*/*file*	/httpcertfile-[*drive*:]*dir**file* /httpcertfile-*svr**sharename**dir**file*
Example:	--httpcertfile /certs/gw.crt	/httpcertfile-\ssl\gw.crt /httpcertfile-m:\ssl\gw.crt /httpcertfile-\\\\server2\c\ssl\gw.crt

See also --httpssl.

--httpmonpassword

Specifies the password for the Monitor console to prompt for before allowing a user to display the Monitor console. Do not use an existing LDAP directory password because the information passes over the non-secure connection between your web browser and the Monitor Agent. See “Securing the Monitor Web Console” on page 647.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpmonpassword *unique_password*	/httpmonpassword-*unique_password*
Example:	--httpmonpassword WatchIt	/httpmonpassword-WatchIt

See also --httpmonuser.

--httpmonuser

Specifies the user name for the Monitor console to prompt for before allowing a user to display the Monitor console. Providing a user name is optional. Do not use an existing LDAP directory user name because the information passes over the non-secure connection between your web browser and the Monitor Agent. See “Securing the Monitor Web Console” on page 647.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpmonuser *unique_user_name*	/httpmonuser-*unique_user_name*
Example:	--httpmonuser MonAdmin	/httpmonuser-MonAdmin

See also --httpmonpassword.

--httpport

Sets the HTTP port number used for the Monitor Agent to communicate with your web browser. The default is 8200; the setting must be unique. See “Configuring the Monitor Agent for HTTP” on page 644.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpport *port_number*	/httpport-*port_number*
Example:	--httpport 8201	/httpport-9200

--httpssl

Enables secure SSL communication between the Monitor Agent and the Monitor console displayed in your web browser. See “Securing the Monitor Web Console” on page 647.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpssl	/httpssl

See also --httpcertfile.

--ipa

Specifies the network address (IP address or DNS hostname) of a server where an MTA is running. The Monitor Agent can communicate with the MTA to obtain information about agents to monitor.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--ipa *network_address*	/ipa-*network_address*
Example:	--ipa 172.16.5.19 --ipa server2	/ipa-172.16.5.20 /ipa-server3

See also --ipp.

--ipp

Specifies the TCP port number associated with the network address of an MTA with which the Monitor Agent can communicate to obtain information about agents to monitor. Typically, the MTA listens for service requests on port 7100.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--ipp *port_number*	/ipp-*port_number*
Example:	--ipp 7110	/ipp-7111

See also --ipa.

--lang

Specifies the language to run the Monitor Agent in, using a two-letter language code. You must install the Monitor Agent in the selected language in order for the Monitor Agent to display in the selected language.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--lang *code*	/lang-*code*
Example:	--lang de	/lang-fr

See Chapter 7, “Multilingual GroupWise Systems,” on page 85 for a list of language codes.

--log

Specifies the full path of the folder where the Monitor Agent writes its log files. The default location varies by platform:

Linux: `/var/log/novell/groupwise/gwmon`

Windows: `c:\ProgramData\Micro Focus\GroupWise Monitor`

NOTE: On some versions of Windows Server, the `ProgramData` folder is not visible by default. To display it in File Explorer, click **View**, then select **Hidden items**.

See "Configuring Monitor Agent Log Settings" on page 647.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--log /*dir*/*file*	/log-[*drive*:]*dir**file* /log-*svr**sharename**dir**file*
Example:	--log /opt/novell/groupwise/agents/logs	/log-\gw\logs /log-m:\gw\logs /log-\\\\server2\c\gw\logs

--monwork

Specifies the location where the Monitor Agent creates its working folder. The default location varies by platform.

Linux: `/tmp/gwmon`

Windows: `c:\Program Files\Micro Focus\GroupWise Server\Monitor`

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--monwork /*folder*	/monwork-[*svr*\\][*vol*:]*dir* /monwork-*svr**vol**dir* /monwork-[*drive*:]*dir* /monwork-*svr**sharename**dir*
Example:	--monwork /tmp	/monwork-\temp /monwork-mail:\ temp /monwork-server2\mail:temp /monwork-\\\\server2\mail\ temp /monwork-\ temp /monwork-m:\temp /monwork-\\\\server2\c\mail\temp

--nosnmp

Disables SNMP for the Monitor Agent. The default is to have SNMP enabled. See "Configuring the Monitor Agent for SNMP" on page 644.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--nosnmp	/nosnmp

--pollthreads

Specifies the number of threads that the Monitor Agent uses for polling the agents for status information. Valid values range from 1 to 32. The default is 20. See "Configuring Polling of Monitored Agents" on page 645.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--pollthreads *number*	/pollthreads-*number*
Example:	--pollthreads 10	/pollthreads-32

--proxy

Routes all communication through the Monitor Agent and the Monitor Application (on the web server). As long as the web server can be accessed through the firewall, the Monitor console can receive information about all GroupWise agents that the Monitor Agent knows about. Without --proxy, the Monitor console cannot communicate with the GroupWise agents through a firewall. See "Configuring Proxy Service Support for the Monitor Console" on page 648.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--proxy	/proxy

--tcpwaitconnect

Sets the maximum number of seconds the Monitor Agent waits for a connection to a monitored agent. The default is 5.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--tcpwaitconnect *seconds*	/tcpwaitconnect-*seconds*
Example:	--tcpwaitconnect 10	/tcpwaitconnect-15

XVI Security Administration

- Chapter 88, “Native GroupWise Security,” on page 685
- Chapter 89, “GroupWise Passwords,” on page 687
- Chapter 90, “Encryption and Certificates,” on page 693
- Chapter 91, “LDAP Directories,” on page 699
- Chapter 92, “Message Security,” on page 701
- Chapter 93, “GroupWise Address Book Security,” on page 703
- Chapter 94, “Spam Protection,” on page 705
- Chapter 95, “Virus Protection,” on page 707

See also Part XIX, “Security Policies,” on page 709.

For additional assistance in managing your GroupWise system, see GroupWise Best Practices (http://wiki.novell.com/index.php/GroupWise).

88 Native GroupWise Security

By default, GroupWise native encryption is employed throughout your GroupWise system. This means that all files related to GroupWise items are automatically encrypted when they are stored on disk. In addition, all connections between the GroupWise client and GroupWise agents use a proprietary, encrypted protocol.

By default, the GroupWise client runs in Online mode, so that all files related to mailboxes are stored on the GroupWise server where the POA for the post office runs. As an administrator, you can chose whether to allow users to set up their mailboxes to use Caching mode or Remote mode, where mailboxes are located on users' workstations.

If you decide to allow users to use Caching mode or Remote mode, the mailbox files on users' workstations are all protected by GroupWise native encryption.

The following sections help you configure your GroupWise system for even tighter security:

- "Mailbox Passwords" on page 687
- "Agent Passwords" on page 691
- "Personal Digital Certificates, Digital Signatures, and S/MIME Encryption" on page 693
- "Server Certificates and SSL Encryption" on page 695
- "Trusted Root Certificates and LDAP Authentication" on page 698

See also Part XIX, "Security Policies," on page 709.

89 GroupWise Passwords

Access to GroupWise mailboxes is protected by post office security settings or GroupWise passwords. Agent passwords grant access to remote servers and protect access to GroupWise agent status information.

- "Mailbox Passwords" on page 687
- "Agent Passwords" on page 691

See also Part XIX, "Security Policies," on page 709.

Mailbox Passwords

When you are setting up a new GroupWise system, you need to determine what kind of password protection you want to have on users' GroupWise mailboxes before users start running GroupWise. In the GroupWise Admin console, you can choose where password information is obtained when users log in to GroupWise, and you can set defaults under Client Options to enforce your choices. You and GroupWise client users should keep in mind that GroupWise passwords are case sensitive.

- "Using Post Office Security Instead of GroupWise Passwords" on page 687
- "Requiring GroupWise Passwords" on page 688
- "Managing GroupWise Passwords" on page 688
- "Using LDAP Passwords Instead of GroupWise Passwords" on page 690
- "Bypassing GroupWise Passwords with Single Sign-On" on page 690
- "Bypassing GroupWise Passwords to Respond to Corporate Mandates" on page 691

Using Post Office Security Instead of GroupWise Passwords

When you create a new post office, you must select a security level for it.

If you select GroupWise Authentication (the default), you can set a default password on mailboxes. For instructions, see "Establishing a Default Password for All New GroupWise Accounts" on page 453. Users can then set their own passwords after they log in.

If you select **GroupWise Authentication** and also select **Allow Login from users with No Password**, you create passwordless mailboxes. This is not recommended except for testing purposes.

If you select **LDAP Authentication** for the post office, users are still not required to set passwords on their GroupWise mailboxes, but they are required to be successfully logged in to a network before they can access their mailboxes.

Requiring GroupWise Passwords

Users are required to set passwords on their GroupWise mailboxes if they want to access their GroupWise mailboxes in any of the following ways:

- Using Caching mode or Remote mode in the GroupWise client
- Using their web browsers and GroupWise WebAccess
- Using an IMAP email client

Managing GroupWise Passwords

When GroupWise passwords are used in addition to network passwords, there are a variety of things you can do to make GroupWise password management easier for you and to make the additional GroupWise password essentially transparent for your GroupWise users.

- "Establishing a Default GroupWise Password for New Accounts" on page 688
- "Accepting eDirectory Authentication Instead of GroupWise Passwords" on page 688
- "Using Micro Focus SecureLogin to Handle GroupWise Passwords" on page 689
- "Using Intruder Detection" on page 689
- "Resetting GroupWise Passwords" on page 689
- "Synchronizing GroupWise Passwords and LDAP Passwords" on page 690
- "Helping Users Who Forget Their Passwords" on page 690

NOTE: A GroupWise password can contain as many as 64 characters and can contain any typeable characters.

Establishing a Default GroupWise Password for New Accounts

If you want to require users to have GroupWise passwords on their mailboxes, you can establish the initial passwords when you create the GroupWise accounts. In the GroupWise Admin console, you can establish a default mailbox password to use automatically on all new GroupWise accounts. For more information, see "Establishing a Default Password for All New GroupWise Accounts" on page 453. Or you can set the password on each new GroupWise account as you create it.

Keep in mind that some situations require users to have passwords on their GroupWise mailboxes, as listed in "Requiring GroupWise Passwords" on page 688.

Accepting eDirectory Authentication Instead of GroupWise Passwords

When you create users in NetIQ eDirectory, you typically assign them network passwords, which users must provide when they log in to the network. If you want to make it easy for client users to access their GroupWise mailboxes, you can select **Use eDirectory Authentication Instead of Password** (GroupWise Admin console > Domain object, Post Object, or User object > **Client Options > Security > Password**). This allows GroupWise users to select **No Password Required with eDirectory** (GroupWise client > **Tools > Options > Security > Password**).

NOTE: This option is not available in GroupWise WebAccess.

As long as users who select this option are logged into eDirectory as part of their network login, they are not prompted by GroupWise for a password when they access their GroupWise mailboxes. If they are not logged in to eDirectory, they must provide their GroupWise passwords in order to access their GroupWise mailboxes.

Using Micro Focus SecureLogin to Handle GroupWise Passwords

If users have Micro Focus SecureLogin installed on their workstations, you can select **Enable single sign-on** (GroupWise Admin console > Domain object, Post Office object, or User object > **Client Options > Security > Password**). This allows GroupWise users to select **Use Single Sign-On** (GroupWise client > **Tools > Options > Security > Password**). Users need to provide their GroupWise mailbox password only once and thereafter SecureLogin provides it for them as long as they are logged in to NetIQ eDirectory.

NOTE: This option is not available in GroupWise WebAccess.

Using Intruder Detection

Intruder detection identifies system break-in attempts in the form of repeated unsuccessful logins. If someone cannot provide a valid user name and password combination within a reasonable time, then that person probably does not belong in your GroupWise system.

Intruder detection for the GroupWise client is performed by the POA and is configurable. You can set the number of failed login attempts before lockout, the length of the lockout, and so on. If a user is locked out, you can re-enable his or her account in the GroupWise Admin console. See "Configuring Intruder Detection" on page 153.

Intruder detection for the GroupWise WebAccess is built in and is not configurable. After five failed login attempts, the user is locked out for 10 minutes. If a user is locked out, the user must wait for the lockout period to end.

Resetting GroupWise Passwords

You can remove a user's password from his or her mailbox if the password has been forgotten and needs to be reset (GroupWise Admin console > User object > **Client Options > Security > Password**). If necessary, you can remove the passwords from all mailboxes in a post office (GroupWise Admin console > Post Office object > **Maintenance > Mailbox/Library Maintenance > Reset Client Options**) This resets all or users' client options settings, not just the passwords.

It is easy for GroupWise users to reset their own passwords (GroupWise client > **Tools** > **Options** > **Security** > **Password**). However, if this method is used when users are in Caching or Remote mode, this changes the password on the local Caching or Remote mailboxes, but does not change the password on the Online mailboxes. To change the Online mailbox password while in Caching or Remote mode, users must use a method they might not be familiar with (GroupWise client > **Accounts > Account Options > Micro Focus GroupWise Account > Properties > Advanced > Online Mailbox Password**).

It is also easy for GroupWise WebAccess users to reset their own passwords (WebAccess > **Options > Password**). However, you might not want users to be able to reset their GroupWise passwords from web browsers. See "Preventing Users from Changing Their GroupWise Passwords in WebAccess" on page 613. GroupWise client users cannot be prevented from changing their GroupWise passwords.

Synchronizing GroupWise Passwords and LDAP Passwords

There is no automatic procedure for synchronizing GroupWise passwords and LDAP passwords. However, if you use LDAP authentication, synchronization becomes a moot point because GroupWise users are authenticated through an LDAP directory such as NetIQ eDirectory and Microsoft Active Directory, rather than by using GroupWise passwords. See "Using LDAP Passwords Instead of GroupWise Passwords" on page 690.

Helping Users Who Forget Their Passwords

The WebAccess Login page includes a **Can't log in** link, which provides the following information to WebAccess users by default:

```
If you have forgotten your GroupWise password, contact your local GroupWise
administrator.
```

For your convenience and for the convenience of your WebAccess users, you can customize the information that is provided by the **Can't log in** link. For set instructions, see "Helping Users Who Forget Their GroupWise Passwords" on page 613.

Using LDAP Passwords Instead of GroupWise Passwords

Instead of using GroupWise passwords, users' password information can be validated using an LDAP directory. In order for users to use their LDAP passwords to access their GroupWise mailboxes, you must define one or more LDAP servers in your GroupWise system and configure the POA for each post office to perform LDAP authentication. For more information, see "Providing LDAP Authentication for GroupWise Users" on page 153.

When LDAP authentication is enabled, you can control whether users can use the GroupWise client to change their LDAP passwords (GroupWise Admin console > **System** > **LDAP Servers** > *select an LDAP object* > **LDAP Authentication** tab > **Disable LDAP Password Changing**). If you allow them to, GroupWise users can change their passwords through the Security Options dialog box (GroupWise client > **Tools > Options > Security**) or on the Passwords page (GroupWise WebAccess > **Options > Password**). If you do not allow them to change their LDAP passwords in the GroupWise client, users must use a different application in order to change their LDAP passwords.

You and users can use some of the same methods to bypass LDAP passwords as you can use for bypassing GroupWise passwords. See "Accepting eDirectory Authentication Instead of GroupWise Passwords" on page 688.

For more information about LDAP passwords, see "Authenticating to GroupWise with Passwords Stored in an LDAP Directory" on page 699.

Bypassing GroupWise Passwords with Single Sign-On

For single sign-on information, see Chapter 54, "Configuring Single Sign-On," on page 477.

Bypassing GroupWise Passwords to Respond to Corporate Mandates

Sometimes it is necessary to access user mailboxes to meet corporate mandates such as virus scanning, content filtering, or email auditing that might be required during litigation. These types of mailbox access are obtain using trusted applications, which are third-party programs that can log into POAs in order to access GroupWise mailboxes. For more information about a using trusted application to bypass mailbox passwords, see "Trusted Applications" on page 64

Agent Passwords

Agent passwords facilitate access to remote servers where restore areas and document storage areas are located. They also protect the agent consoles and GroupWise Monitor from unauthorized access.

- "Facilitating Access to Remote Servers" on page 691
- "Protecting the Agent Consoles" on page 691
- "Protecting the GroupWise Monitor Console" on page 692

Facilitating Access to Remote Servers

The Windows POA needs user name and password information in order to access a restore area or a document storage area on a server other than the one where the post office folder structure is located. There are two ways to provide this information:

- Fill in the **Remote User Name** and **Remote Password** fields (GroupWise Admin console > Post Office object > **Settings**)
- Add the /user and /password startup switches to the POA startup file to provide a user name and password

Providing passwords in clear text in a startup file might seem like a security risk. However, the servers where the agents run should be kept physically secure. If an unauthorized person did gain physical access, they would not be doing so for the purpose of obtaining these particular passwords. The passwords are encrypted as they pass over the wire between servers, so the security risk is minimal.

Protecting the Agent Consoles

When you install the GroupWise agents, they are automatically configured with an agent console, and no password protection is provided. If you do not want agent console status information available to anyone who knows the agent network address and port number, you should set passwords on your agent consoles. For instructions, see:

- "Using the POA Console" on page 163
- "Using the MTA Console" on page 237
- "Using the GWIA Console" on page 311
- "Using the DVA Console" on page 373
- "Using the WebAccess Application Console" on page 621

If you plan to access the GroupWise Monitor consoles, it is most convenient if you use the same password on all agent consoles. That way, you can provide the agent console password once in GroupWise Monitor, rather than having to provide various passwords as you view the consoles for various agents. For information about providing the agent console password in GroupWise Monitor, see "Configuring Polling of Monitored Agents" on page 645.

Protecting the GroupWise Monitor Console

Along with the agent consoles, you can also provide password protection for the Monitor console itself, from which all the agent consoles can be accessed. For instructions, see "Securing the Monitor Web Console" on page 647.

90 Encryption and Certificates

GroupWise native encryption is employed throughout your GroupWise system. For background information, see Chapter 88, "Native GroupWise Security," on page 685. Additional security measures should also be utilized to secure your GroupWise data.

- "Personal Digital Certificates, Digital Signatures, and S/MIME Encryption" on page 693
- "Server Certificates and SSL Encryption" on page 695
- "Trusted Root Certificates and LDAP Authentication" on page 698

See also Part XIX, "Security Policies," on page 709.

Personal Digital Certificates, Digital Signatures, and S/MIME Encryption

If desired, you can implement S/MIME encryption for GroupWise client users by installing various security providers on users' workstations, including:

- Entrust 4.0 or later (http://www.entrust.com)
- Microsoft Base Cryptographic Provider 1.0 or later (included with Internet Explorer 4.0 or later)
- Microsoft Enhanced Cryptographic Provider 1.0 or later (http://msdn.microsoft.com/en-us/library/windows/desktop/aa386986(v=vs.85).aspx)
- Microsoft Strong Cryptographic Provider (http://msdn.microsoft.com/en-us/library/windows/desktop/aa386989(v=vs.85).aspx)
- Gemalto Smart Card 2.0 or later (http://www.gemalto.com/gemplus/index.html)
- Schlumberger Cryptographic Provider (http://www.slb.com)

For additional providers, consult the Micro Focus Partner Product Guide (http://www.novell.com/partnerguide/).

These products enable users to digitally sign and encrypt their messages using S/MIME encryption. When a sender digitally signs a message, the recipient is able to verify that the item was not modified en route and that it originated from the sender specified. When a sender encrypts a message, the sender ensures that the intended recipient is the only one who can read it. Digitally signed and encrypted messages are protected as they travel across the Internet, but native GroupWise encryption is removed as messages leave your GroupWise system.

After users have installed an S/MIME security provider on their workstations, you can configure default functionality for it (GroupWise Admin console > Domain object, Post Office object, or User object > **Client Options > Send > Security > Secure Item Options**). You can specify a URL from which you want users to obtain their S/MIME certificates. You can require the use of digital signatures and encryption, rather than letting users decide when to use them. You can even select the encryption algorithm and encryption key size if necessary. For more information, see "Send Options: Security" on page 572.

After you have configured S/MIME functionality in the GroupWise Admin console, GroupWise users must select the security provider (GroupWise client > **Tools > Options > Security > Send Options**) and then obtain a personal digital certificate. Unless you installed Entrust, users can request

certificates (GroupWise client > **Tools > Options > Certificates > Get Certificate**). If you provided a URL, users are taken to the certificate authority of your choice. Otherwise, certificates for use with GroupWise can be obtained from various certificate providers, including:

- Micro Focus, Inc. (if you have installed Micro Focus Certificate Server 2 or later (http://www.novell.com/solutions/identity-and-security/?redir=products/certserver))
- VeriSign, Inc. (http://www.verisign.com)
- Thawte Certification (http://www.thawte.com)
- GlobalSign (https://www.globalsign.com)

NOTE: Some certificate providers charge a fee for certificates and some do not.

After users have selected the appropriate security provider and obtained a personal digital certificate, they can protect their messages with S/MIME encryption by digitally signing them (GroupWise client > **Actions > Sign Digitally**) and encrypting them (GroupWise client > **Actions > Encrypt**). Buttons are added to the GroupWise toolbar for convenient use on individual messages, or users can configure GroupWise to always use digital signatures and encryption (GroupWise client > **Tools > Options > Security > Send Options**). The messages they send with digital signatures and encryption can be read by recipients using any other S/MIME-enabled email product.

GroupWise client users are responsible for managing their personal digital certificates. Users can have multiple personal digital certificates. In the GroupWise client, users can view their own certificates, view the certificates they have received from their contacts, access recipient certificates from LDAP directories, change the trust level on certificates, import and export certificates, and so on. For more information, see “Accessing S/MIME Certificates in an LDAP Directory” on page 700.

The certificates are stored in the local certificate store on the user’s workstation. They are not stored in GroupWise. Therefore, if a user moves to a different workstation, he or she must import the personal digital certificate into the certificate store on the new workstation, even though the same GroupWise account is being accessed.

If your system includes smart card readers on users’ workstations, certificates can also be retrieved from this source, so that after composing a message, users can sign them by inserting their smart cards into the card readers. The GroupWise client picks up the digital signature and adds it to the message.

The GroupWise client verifies the user certificate to ensure that it has not been revoked. It also verifies the certificate authority. If a certificate has expired, the GroupWise user receives a warning message.

For complete details about using S/MIME encryption in the GroupWise client, see “Sending S/MIME Secure Messages” in the *GroupWise 18 Client User Guide*.

NOTE: S/MIME encryption is not available in GroupWise WebAccess.

Any messages that are not digitally signed or encrypted are still protected by native GroupWise encryption as long as they are within your GroupWise system.

Server Certificates and SSL Encryption

You should strengthen native GroupWise encryption with Secure Sockets Layer (SSL) communication between servers where GroupWise agents are installed. You can choose to purchase a server certificate from a commercial certificate authority (CA) or you can use a self-signed certificate provided by the GroupWise certificate authority.

The advantage of using a self-signed certificate is that you can proceed to set up SSL immediately, without waiting to the certificate from a certificate authority. However, the first time the GroupWise client encounters the self-signed certificate, it prompts the user to accept the certificate. The advantage of a commercially generated certificate is that the GroupWise client accepts it automatically. You might choose to use a self-signed certificate initially, while you are waiting to obtain a commercially generated certificate.

If you have not already set up SSL on your system, obtain a certificate for each GroupWise server, then configure the agents to use SSL:

- "Using a Self-Signed Certificate from the GroupWise Certificate Authority" on page 695
- "Using a Commercially Signed Certificate" on page 695
- "Configuring the Agents to Use SSL" on page 697

If you have already set up SSL on your system and are using it with other applications in addition to GroupWise, skip to "Configuring the Agents to Use SSL" on page 697.

Using a Self-Signed Certificate from the GroupWise Certificate Authority

The GroupWise certificate authority is managed by using the GroupWise Administration Utility (GWAdminUtil). Use the following commands:

Task	GroupWise Admin Utility Command
Generate a new server certificate for a domain server	`gwadminutil ca -i` */path_to_domain_folder*
Generate a new server certificate for a post office server	`gwadminutil ca -i` */path_to_domain_folder*
List existing certificates and serial numbers	`gwadminutil ca -l`
Display detailed information about a certificate	`gwadminutil ca -p` *serial_number*
Revoke a certificate	`gwadminutil ca -r` *serial_number*

For more information, see gwadminutil ca in the *GroupWise 18 Utilities Reference*

Using a Commercially Signed Certificate

In order to purchase a commercially signed certificate, you must create a certificate signing request (CSR).

- "Generating a Certificate Signing Request" on page 696
- "Submitting the Certificate Signing Request to a Certificate Authority" on page 697

Generating a Certificate Signing Request

The certificate signing request (CSR) includes the hostname of the server where the agents run. Therefore, you must create a CSR for every server where you want the GroupWise agents to use SSL. However, all GroupWise agents running on the same server can all use the same certificate, so you do not need separate CSRs for different agents. The CSR also includes your choice of name and password for the private key file that must be used with each certificate. This information is needed when configuring the agents to use SSL.

- "Linux: Using OpenSSL" on page 696
- "Windows Server 2008/2012: Using IIS Manager" on page 696

Linux: Using OpenSSL

For background information, see HOWTO Certificates (http://www.openssl.org/docs/HOWTO/certificates.txt).

1 Open a terminal window, become `root`, and change to a convenient folder where you want to create the CSR.

2 Enter the following command to create a private key file:

```
openssl genrsa -out key_file_name.key 2048
```

Replace *key_file_name.key* with a convenient name for the private key file, such as `gw.key`.

3 Create the CSR:

 3a Enter the following command:

```
openssl req -new -key key_file_name.key -out csr_file_name.csr
```

 Replace *key_file_name*`.key` with the key file that you created in Step 2.

 3b Enter the two-letter code for your country, such as `US` for the United States, `DE` for Germany, and so on.

 3c Enter your state or province.

 3d Enter your city.

 3e Enter the name of your company or organization.

 3f Enter your department or other organizational unit.

 3g Enter the fully qualified domain name of the server for which you are obtaining a certificate, such as `gw3.novell.com`.

 3h Enter the email address of a contact person for that server.

 3i (Optional) Enter a password for the CSR.

 3j (Optional) Enter a secondary name for your company or organization.

4 Skip to "Submitting the Certificate Signing Request to a Certificate Authority" on page 697.

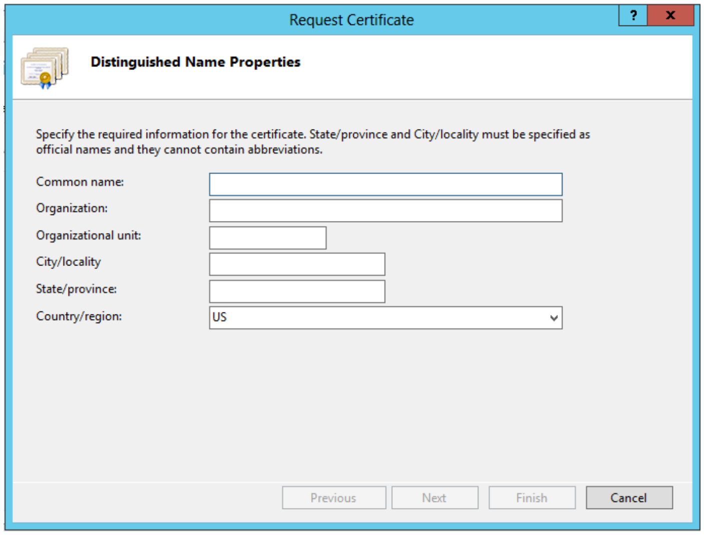
Windows Server 2008/2012: Using IIS Manager

1 Open IIS Manager.

2 In the **Connections** pane, click the server to display the server Home view.

3 In the **Features View**, double-click **Server Certificates**.

4 In the **Actions** pane, click **Create Certificate Request**.



5 In the **Common Name** field, specify the fully qualified domain name of the server for which you are obtaining a certificate, such as `gw3.novell.com`.

6 Fill in the rest of the fields with the requested information, then click **Next**.

7 The default cryptographic service provider and bit length are acceptable, so click **Next**.

8 Specify a name for the CSR file, such as `gw.csr`, then click **Finish**.

If you do not specify a full path name, the CSR file is created in the `c:\Windows\System32` folder.

9 Continue with Submitting the Certificate Signing Request to a Certificate Authority.

Submitting the Certificate Signing Request to a Certificate Authority

To obtain a server certificate, you can submit the certificate signing request (*`server_name`*`.csr` file) to a certificate authority. If you have not previously used a certificate authority, you can use the keywords “certificate authority” to search the web for certificate authority companies.

The process of submitting the CSR varies from company to company. Most provide online submission of the request. Follow their instructions for submitting the request. The certificate authority must be able to provide the certificate in Base64/PEM or PFX format.

Configuring the Agents to Use SSL

To configure the agents to use SSL you must first enable them for SSL and then provide certificate and key file information. For detailed instructions, see the following sections:

- “Securing the Post Office with SSL Connections to the POA” on page 152
- “Securing the Domain with SSL Connections to the MTA” on page 229
- “Securing Internet Access with SSL Connections to the GWIA” on page 271
- “Securing Document Conversion with SSL Connections” on page 371

Trusted Root Certificates and LDAP Authentication

LDAP authentication, relies on the presence of a trusted root certificate (often named `rootcert.der`) located on your LDAP server. For more information, see “Providing LDAP Authentication for GroupWise Users” on page 153.

A trusted root certificate is automatically created for a server when you install an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory on that server.

91 LDAP Directories

LDAP (Lightweight Directory Access Protocol) is a standard Internet protocol for accessing commonly used network directories. If you are new to GroupWise or LDAP, you might find it useful to review TID 2955731, "GroupWise and LDAP," in the Micro Focus Support Knowledgebase (http://www.novell.com/support/). This TID provides an overview of LDAP and explains the two address-book-related ways that GroupWise makes use of LDAP.

This section briefly summarizes the address book usages of LDAP, and explains how LDAP can also be used to store security information such as passwords and certificates for use with GroupWise.

- "Accessing Public LDAP Directories from GroupWise" on page 699
- "Authenticating to GroupWise with Passwords Stored in an LDAP Directory" on page 699
- "Accessing S/MIME Certificates in an LDAP Directory" on page 700

See also Part XIX, "Security Policies," on page 709.

Accessing Public LDAP Directories from GroupWise

The GroupWise client uses LDAP to provide access to directory services such as Bigfoot. This enables GroupWise users to select email addresses from these popular directory services and add them to their personal GroupWise address books. See "Using the LDAP Address Book" in the *GroupWise 18 Client User Guide*.

Authenticating to GroupWise with Passwords Stored in an LDAP Directory

Enabling LDAP authentication for the POA is independent of these LDAP address book features. You need to enable LDAP authentication when you want the POA to authenticate the user's password in an LDAP directory such as NetIQ eDirectory or Microsoft Active Directory, rather than looking for a password in the user's GroupWise account information. The POA can make use of the following LDAP capabilities:

- "Access Method" on page 699
- "LDAP User Name and Password" on page 700

When you understand these LDAP capabilities, you are ready to set up LDAP authentication for your GroupWise users. See "Providing LDAP Authentication for GroupWise Users" on page 153.

Access Method

On a server-by-server basis (GroupWise Admin console > **System > LDAP Servers > LDAP Authentication**), you can specify whether you want each LDAP server to respond to authentication requests using a bind or a compare.

- **Bind:** With a bind, the POA essentially logs in to the LDAP server. When responding to a bind request, most LDAP servers enforce password policies such as grace logins and intruder lockout, if such policies have been implemented by the LDAP directory.

* **Compare:** With a compare, the POA provides the user password to the LDAP server. When responding to a compare request, the LDAP server compares the password provided by the POA with the user's password in the LDAP directory, and returns the results of the comparison. Using a compare connection can provide faster access because there is typically less overhead involved because password policies are not being enforced.

Regardless of whether the POA is submitting bind requests or compare requests to authenticate GroupWise users, the POA can stay connected to the LDAP server as long as authentication requests continue to occur before the connection times out. This provides quick response as users are accessing their mailboxes.

LDAP User Name and Password

On each LDAP directory that you configure (GroupWise Admin console > **System > LDAP Severs > LDAP Authentication**), you can decide what user name you want the POA to use when accessing the LDAP server.

* **LDAP User Login:** If you want the POA to access the LDAP server with specific rights to the LDAP directory, you can provide a user name and password for the POA to use when logging in. The rights of the user determine what information in the LDAP directory will be available during the authentication process.
* **Public or Anonymous Login:** If you do not provide a specific LDAP user name and password as part of the LDAP configuration information, then the POA accesses the LDAP directory with a public or anonymous connection. Only public information is available when using such a login.

Accessing S/MIME Certificates in an LDAP Directory

Just as the POA can access user password information in an LDAP directory, the GroupWise client can access recipients' digital certificates in an LDAP directory. See "Using LDAP to Search for Recipient Encryption Certificates" in the *GroupWise 18 Client User Guide*.

When a certificate is stored on an LDAP server, the GroupWise client searches the LDAP server every time the certificate is used. Certificates from LDAP servers are not downloaded into the local certificate store on the user's workstation.

To facilitate this process, the user must select a default LDAP directory in the LDAP address book (GroupWise client > **Address Book > Micro Focus LDAP Address Book > Directories > Set as Default**) and enable searching (GroupWise client > **Tools > Options > Security > Send Options > Advanced Options > Search for recipient encryption certificates in the default LDAP directory defined in LDAP Address Book**).

An advantage to this is that recipients' certificates are available no matter what workstation the GroupWise user sends the message from.

NOTE: This feature is not available in GroupWise WebAccess.

---

92 Message Security

The GroupWise client accommodates users' preferences for security and privacy when sending messages. Users can do the following:

- Sign a message with standardized text (GroupWise client > **Tools** > **Options** > **Environment** > **Signature**).
- Sign a message with an electronic business card (vCard) (GroupWise client > **Tools > Options > Environment > Signature**).
- Digitally sign and encrypt a message. See "Personal Digital Certificates, Digital Signatures, and S/MIME Encryption" on page 693.
- Give a message a security classification (GroupWise client > **New Mail > Send Options > General > Classification > Normal, Proprietary, Confidential, Secret, Top Secret, or For your eyes only**).
- Conceal the subject of an email message (GroupWise client > **New Mail > Send Options > Security > Conceal subject**).
- Mark messages and appointments private so that proxy users cannot see them. (GroupWise client > **Actions > Mark Private**).
- Attach a password-protected document to a message and have the application prompt the recipient to supply the password before the recipient can open the document
- Require a password in order to mark a Routing Slip completed (GroupWise client > **Tools > Options > Security > Send Options > Require password to complete routed item**). This can prevent a user who is proxied to the mailbox from marking the item completed, or if multiple users proxy to the mailbox, it can be used to ensure that only the user for whom the item was intended can complete it.

In addition, if the users in your GroupWise system exchange messages with users in other GroupWise systems, you can set preferences to control what types of information pass between the two systems. For example, you can prevent external GroupWise users from performing busy searches or obtaining message delivery status. See "External Access Rights" on page 58.

See also Part XIX, "Security Policies," on page 709.

93 GroupWise Address Book Security

One of the purposes of the GroupWise Address Book is to make user information available to all GroupWise users. However, there might be types of information that you do not want to display.

- "LDAP Directory Information Displayed in the GroupWise Address Book" on page 703
- "Suppressing the Contents of the User Description Field" on page 703
- "Controlling GroupWise Object Visibility in the GroupWise Address Book" on page 704
- "Controlling GroupWise Object Visibility between GroupWise Systems" on page 704

See also Part XIX, "Security Policies," on page 709.

LDAP Directory Information Displayed in the GroupWise Address Book

If you imported GroupWise users from the LDAP directory such as NetIQ eDirectory or Microsoft Active Directory, the GroupWise Address Book displays information stored in the LDAP directory for users, resources, and groups in your GroupWise system. By default, the following information is displayed:

- Name
- Office phone number
- Department
- Fax number
- User name

You can configure the GroupWise Address Book to display more or less information to meet the needs of your users. See "Customizing Address Book Fields" on page 69.

Suppressing the Contents of the User Description Field

By default, when you display details about a user in the GroupWise Address Book, the information in the **Description** field of the User object is displayed. If you keep confidential information in the **Description** field of the User object, you can prevent this information from appearing the GroupWise Address Book. See "Preventing the User Description Field from Displaying in the Address Book" on page 72.

Controlling GroupWise Object Visibility in the GroupWise Address Book

You might need to create users, resources, or groups that are not available to all GroupWise users. You can accomplish this by restricting the set of users that can see such objects in the GroupWise Address Book. You can make such objects visible only to the members of a domain, only to the members of a post office, or to no one at all. An object does not need to be visible to be addressable. For instructions, see "Controlling Object Visibility" on page 72.

Controlling GroupWise Object Visibility between GroupWise Systems

If you synchronize your GroupWise system with other GroupWise systems to simplify addressing for users of both systems, you can control what information from your GroupWise Address Book you want to be available in the Address Books of other GroupWise systems. For instructions, see "Synchronizing User Information between External GroupWise Systems" on page 115.

94 Spam Protection

Unwanted Internet email messages (spam) can be a distracting nuisance to GroupWise client users. Your first line of defense against spam is the Internet Agent (GWIA). Your second line of defense is the Junk Mail Handling feature of the GroupWise client.

- "Configuring the GWIA for Spam Protection" on page 705
- "Configuring the GroupWise Client for Spam Protection" on page 705

See also Part XIX, "Security Policies," on page 709.

Configuring the GWIA for Spam Protection

In the GroupWise Admin console, you can configure the GWIA to reject messages in certain situations:

- Messages are received from known open relay hosts or spam hosts (GroupWise Admin console > GWIA object > **Access Control > Blacklists**).
- Messages are received from any hosts that you specifically do not want to receive messages from (GroupWise Admin console > GWIA object > **Access Control > Default Class of Service > Edit > Allow Incoming Messages, Prevent Incoming Messages, and Exceptions**).
- Messages are received through an anti-spam service that uses an "X" header field to identify potential spam (GroupWise Admin console > GWIA object > **SMTP/MIME > Settings > Junk Mail**).
- Thirty messages are received within 10 seconds from the same sending host (GroupWise Admin console > GWIA object > **SMTP/MIME Settings > Security Settings**). The number of message and the time interval can be modified to identify whatever you consider to be a potential mailbomb.
- Messages are received from SMTP hosts that are not using the AUTH LOGIN host authentication method (--forceinboundauth startup switch).
- The sender's identify cannot be verified (GroupWise Admin console > GWIA object > **SMTP/MIME Settings > Security Settings**).

For detailed setup instructions on these anti-spam security measures, see "Blocking Unwanted Email from the Internet" on page 285.

Messages that are identified as spam by the GWIA are not accepted into your GroupWise system.

Configuring the GroupWise Client for Spam Protection

The Junk Mail Handling feature (GroupWise client > **Tools > Junk Mail Handling**) provides users with the following options for dealing with unwanted messages that have not been stopped by the GWIA:

- Individual email addresses or entire Internet domains can be placed on the user's Block List. Messages from blocked addresses never arrive in the user's mailbox.

* Individual email addresses or entire Internet Domains can be placed on the user's Junk List. Messages from these addresses are automatically delivered to the Junk Mail folder in the user's mailbox. The user can configure automatic deletion of items in the Junk Mail folder and can also create rules to act on items placed in the Junk Mail folder.
* Messages from users whose addresses are not in the user's personal address books can be automatically delivered to the Junk Mail folder.

The Junk Mail Handling feature in the GroupWise client is enabled by default, although you can control its functionality (GroupWise Admin console > Domain object, Post Office object, or User object > **Client Options > Environment > Junk Mail**).

For detailed usage instructions for the Junk Mail Handling feature in the GroupWise client, see "Handling Unwanted Email (Spam)" in the *GroupWise 18 Client User Guide*.

NOTE: The Junk Mail Handling feature is not available in WebAccess.

---

95 Virus Protection

Virus protection for your GroupWise system is provided by third-party products. For information about security products for use with your GroupWise system, see the Micro Focus Partner Product Guide (http://www.novell.com/partnerguide/) and the Micro Focus Open Enterprise Server Partner Support site (http://www.novell.com/products/openenterpriseserver/partners/).

See also Part XIX, “Security Policies,” on page 709.

XIX Security Policies

- Chapter 96, “Securing GroupWise Data,” on page 711
- Chapter 97, “Securing GroupWise Agents,” on page 713
- Chapter 98, “Securing GroupWise System Access,” on page 717
- Chapter 99, “Secure Migrations,” on page 719

See also Part XVIII, “Security Administration,” on page 683.

96 Securing GroupWise Data

- "Limiting Physical Access to GroupWise Servers" on page 711
- "Securing File System Access" on page 711
- "Securing Domains and Post Offices" on page 711

Limiting Physical Access to GroupWise Servers

Servers where GroupWise data resides should be kept physically secure, where unauthorized persons cannot gain access to the server consoles.

Securing File System Access

For data security, encrypted file systems should be used on servers where GroupWise domains, post offices, and agents reside. Only GroupWise administrators should have direct access to GroupWise data.

Securing Domains and Post Offices

In the GroupWise Admin console, administrators in addition to the GroupWise Super Admin should be given rights judiciously. See Chapter 3, "GroupWise Administrators," on page 45.

97 Securing GroupWise Agents

- "Setting Up SSL Connections" on page 713
- "Protecting Agent Consoles" on page 713
- "Protecting Agent Startup Files" on page 713
- "Protecting Agent and Application Log Files" on page 714
- "Preventing the GWIA from Acting as a Relay Host" on page 714
- "Protecting Agent Processes on Linux" on page 714
- "Protecting Trusted Applications" on page 714

Setting Up SSL Connections

All of the GroupWise agents should be configured to use SSL connections:

- "Securing the Post Office with SSL Connections to the POA" on page 152
- "Securing the Domain with SSL Connections to the MTA" on page 229
- "Securing Internet Access with SSL Connections to the GWIA" on page 271
- "Securing Document Conversion with SSL Connections" on page 371
- "Securing the Monitor Web Console" on page 647

GroupWise agents are initially configured with self-signed certificates provided by the GroupWise certificate authority. Publicly signed certificates provide stronger protection. For more information, see "Using a Commercially Signed Certificate" on page 695.

Protecting Agent Consoles

If you do not provide passwords on the GroupWise agent consoles, unauthorized persons can access them by simply knowing the IP address or hostname of the machine where the agent runs, along with the HTTP port the agent is using. Set up GroupWise agent consoles with passwords:

- "Using the POA Console" on page 163
- "Using the MTA Console" on page 237
- "Using the GWIA Console" on page 311
- "Using the DVA Console" on page 373
- "Securing the Monitor Web Console" on page 647

Protecting Agent Startup Files

The startup files for all GroupWise agents should be protected from tampering. See the following sections for the default locations of the agent startup and configuration files:

- Chapter 20, "Using POA Startup Switches," on page 183

* Chapter 26, “Using MTA Startup Switches,” on page 247
* Chapter 34, “Using GWIA Startup Switches,” on page 319
* Chapter 40, “Using DVA Startup Switches,” on page 379
* Chapter 87, “Using Monitor Agent Startup Switches,” on page 675

Protecting Agent and Application Log Files

The log files for all GroupWise agents and applications should be protected against access by unauthorized persons. Some contain very detailed information about your GroupWise system and GroupWise users. See the following sections for the default locations of the agent and application log files:

* “Using POA Log Files” on page 166
* “Using MTA Log Files” on page 238
* “Using GWIA Log Files” on page 312
* “Using DVA Log Files” on page 374
* “Using WebAccess Application Log Files” on page 621
* “Using Calendar Publishing Host Log Files” on page 631
* “Configuring Monitor Agent Log Settings” on page 647
* “Configuring Monitor Application Log Settings” on page 652

Preventing the GWIA from Acting as a Relay Host

Use the GWIA --disallowauthrelay switch to prevent spammers from using GroupWise accounts to authenticate to the GWIA and then using it as a relay host for their spam. The switch has no effect on normal GroupWise account usage in the GroupWise client or WebAccess. However, it does prevent users who access their GroupWise mailboxes from a POP or IMAP client from sending messages to users outside of the GroupWise system, because the GWIA identifies this activity as relaying.

Protecting Agent Processes on Linux

On Linux, the GroupWise agents are installed to run as the `root` user by default. This is not a secure configuration. Immediately after installation, you should set up a non-`root` user for the agents to run as. For more information, see “Running the Linux GroupWise Agents as a Non-root User” in the *GroupWise 18 Installation Guide*.

Protecting Trusted Applications

Trusted applications are third-party programs that can log in to POAs and GWIAs in order to access GroupWise mailboxes. For background information, see “Trusted Applications” on page 64.

Trusted applications log in to GroupWise agents by using trusted application keys that are created when the trusted application is created. It is essential that these keys are protected and not allowed to become public. Steps you can take to protect trusted application keys include:

* Associating the trusted application key with a single IP address whenever possible
* Reviewing third-party log files for sensitive data such as the key before sharing them with others

- Not sharing trusted application keys with others for any reason
- Removing old keys that are no longer needed

98 Securing GroupWise System Access

- "Using a Proxy Server with Client/Server Access" on page 717
- "Using LDAP Authentication for GroupWise Users" on page 717
- "Managing Mailbox Passwords" on page 717
- "Enabling Intruder Detection" on page 717

Using a Proxy Server with Client/Server Access

POAs in your GroupWise system should be located behind your firewall. If GroupWise client users want to access their GroupWise mailboxes from outside your firewall using the GroupWise client, you should set up a proxy server outside your firewall to provide access. For more information, see "Securing Client Access through an External Proxy Server" on page 150.

GroupWise WebAccess users access their GroupWise mailboxes through their web browsers, so your web server handles the access issues for such users.

Using LDAP Authentication for GroupWise Users

LDAP authentication provides a more secure method of mailbox access than standard GroupWise authentication, which is the default when you set up your GroupWise system. Therefore, you should implement LDAP authentication. For instructions, see "Providing LDAP Authentication for GroupWise Users" on page 153.

On the LDAP Directory object, the LDAP user name that you provide on the LDAP **Authentication** tab should be granted only browser rights in the LDAP directory. The password for the LDAP user should be long and randomly generated.

On your LDAP servers, the trusted root certificate file should be write protected so that it cannot be tampered with.

Managing Mailbox Passwords

GroupWise offers varying levels of password security. For more information, see "Mailbox Passwords" on page 687. Ensure that you understand the options available to you, and that you select the level of password security that is appropriate to your GroupWise system.

Enabling Intruder Detection

You can configure the POA to lock out a user that provides the wrong mailbox password too many times. For more information, see "Configuring Intruder Detection" on page 153.

99 Secure Migrations

- "GroupWise Server Migration Utility" on page 719

GroupWise Server Migration Utility

During its operation, the GroupWise Server Migration Utility prompts for some restricted-access information. It also modifies critical GroupWise agent startup files. This section explains why.

- "Source Server Credentials" on page 719
- "Destination Server root Password" on page 719
- "Agent Startup Files" on page 719

For more information about the GroupWise Server Migration Utility, see the *GroupWise Server Migration Guide*.

Source Server Credentials

The Server Migration Utility prompts for a user name and password that provides read/write access to the NetWare or Windows server so that the Linux server can mount the source server with read/write access.

In addition, the Server Migration Utility needs read/write access to the domain or post office folder that is being migrated. Read/write access enables the Server Migration Utility to copy the contents of the post office folder or domain folder, including the post office database and domain database, so that file locking is respected while the data is being copied. File locking prevents database damage.

Destination Server root Password

The Server Migration Utility prompts for the `root` password so that it can mount the NetWare volume or the Windows share to the Linux file system. It also needs the `root` password in order to communicate with the SSH (secure shell) daemon on the Linux server. The SSH daemon allows `root` access for the utility to install the GroupWise RPMs, to run the programs required for migration locally on the Linux server, and to create and save the Linux agent startup files.

In addition, `root` permissions might be required to write the post office or domain data to the Linux server, depending on where the user decided to locate the post office or domain. After the migration, the user can configure the GroupWise agents to run as a non-`root` user for improved security. For more information, see "Running the Linux GroupWise Agents as a Non-root User" in the *GroupWise 18 Installation Guide*.

Agent Startup Files

When the Server Migration Utility migrates an agent, the only change it makes to its startup file is to modify the --home switch to point to the new location of the post office or domain on the Linux server. Existing switch settings are retained, except for paths and IP addresses that would be invalid in the new Linux environment.

XX Appendixes

- Appendix A, “GroupWise Port Numbers,” on page 723
- Appendix B, “GroupWise URLs,” on page 733
- Appendix C, “Linux Basics for GroupWise Administration,” on page 735

A GroupWise Port Numbers

- "Opening Ports for GroupWise Agents and Applications" on page 723
- "Protocol Flow Diagram with Port Numbers" on page 726
- "Post Office Agent Port Numbers" on page 727
- "Message Transfer Agent Port Numbers" on page 728
- "Internet Agent Port Numbers" on page 728
- "Document Viewer Agent Port Numbers" on page 729
- "WebAccess Application Port Numbers" on page 729
- "Calendar Publishing Host Port Numbers" on page 730
- "Monitor Agent Port Number" on page 730
- "Monitor Application Port Numbers" on page 730
- "GroupWise High Availability Service Port Number (Linux Only)" on page 731
- "Port Numbers for Products Frequently Used with GroupWise" on page 731

Opening Ports for GroupWise Agents and Applications

When you install GroupWise agents or applications on a server where a firewall is enabled, you must ensure that the firewall is configured to allow communication on the ports used by the GroupWise agents and applications on the server.

- "Opening Ports on OES Linux" on page 723
- "Opening Ports on SLES" on page 724
- "Opening Ports on Windows" on page 725

Opening Ports on OES Linux

The following procedure is an example of how to open ports through a firewall on Micro Focus Open Enterprise Server (OES). The exact procedure for your specific version of OES might be slightly different.

1 In YaST, click **Security and Users > Firewall**.

2 In the left panel, click **Allowed Services**.

3 (Conditional) To open ports for a web browser for GroupWise WebAccess or for the agent consoles:

  3a In the **Service to Allow** drop-down list, select **HTTP Server** (for a non-secure HTTP connection), then click **Add**.

  3b In the **Service to Allow** drop-down list, select **HTTPS Server** (for a secure SSL connection), then click **Add**.

4 (Conditional) To open ports for the GWIA:

4a In the **Service to Allow** drop-down list, select **IMAP Server** (for a non-secure IMAP connection), then click **Add**.

4b In the **Service to Allow** drop-down list, select **IMAPS Server** (for a secure SSL IMAP connection), then click **Add**.

4c In the **Service to Allow** drop-down list, click **LDAP Server** (for a non-secure LDAP connection), then click **Add**.

4d In the **Service to Allow** drop-down list, click **LDAPS Server** (for a secure LDAP connection), then click **Add**.

4e In the **Service to Allow** drop-down list, click **Mail Server**, then click **Add**.

4f In the **Service to Allow** drop-down list, click **POP3 Server** (for a non-secure POP3 connection) then click **Add**.

4g In the **Service to Allow** drop-down list, click **POP3S Server** (for a secure POP3 connection), then click **Add**.

5 (Conditional) To open ports for the other GroupWise agents:

5a Click **Advanced**.

5b In the **TCP Ports** field, list the port numbers, in a space-delimited list, for the GroupWise agents on this server, as provided in Appendix A, "GroupWise Port Numbers," on page 723.

5c Click **OK**.

6 (Conditional) To open the port for Samba, so that the GroupWise Admin console can access remote restore areas and document storage areas:

6a In the **Service to Allow** drop-down list, click **Samba Server**, then click **Add**.

7 After you have opened all the ports that GroupWise components need to communicate through on this server, click **Next**.

8 Review the list of services and ports that you have configured for this server, then click **Accept**.

Opening Ports on SLES

The following procedure is an example of how to open ports through a firewall on SUSE Linux Enterprise Server (SLES). The exact procedure for your specific version of SLES might be slightly different.

1 In YaST, click **Security and Users > Firewall**.

2 In the left panel, click **Allowed Services**.

3 (Conditional) To open ports for a web browser for GroupWise WebAccess or for the agent consoles:

3a In the **Service to Allow** drop-down list, select **HTTP Server** (for a non-secure HTTP connection), then click **Add**.

3b In the **Service to Allow** drop-down list, select **HTTPS Server** (for a secure SSL connection), then click **Add**.

4 (Conditional) To open ports for the GroupWise agents and applications:

4a Click **Advanced**.

4b In the **TCP Ports** field, list the port numbers, in a space-delimited list, for the GroupWise agents and applications on this server, as provided in Appendix A, "GroupWise Port Numbers," on page 723.

4c Click **OK**.

5 (Conditional) To open ports for Samba, so that the GroupWise Admin console can access remote restore areas and document storage areas:

   5a In the **Service to Allow** drop-down list, select **Samba Client**, then click **Add**.

   5b In the **Service to Allow** drop-down list, click **Samba Server**, then click **Add**.

6 After you have opened all the ports that GroupWise components need to communicate through on this server, click **Next**, then click **Finish**.

Opening Ports on Windows

The following procedure is an example of how to open ports through a firewall on Windows Server. The exact procedure for your specific version of Windows Server might be slightly different.

1 On the **Start** menu, click **Control Panel**, then under **System and Security**, click **Check firewall status**.

2 In the left panel, click **Advanced Settings** to open Windows Firewall with Advanced Security.

3 In the left panel, click **Inbound Rules**.

4 Click **Action > New Rule**.

5 Select **Port**, then click **Next**.

6 Ensure that **TCP** is selected.

7 In the **Specific local ports** field, list the port numbers, in a comma-delimited list, for the GroupWise agents and applications on this server, as provided in this appendix, then click **Next**.

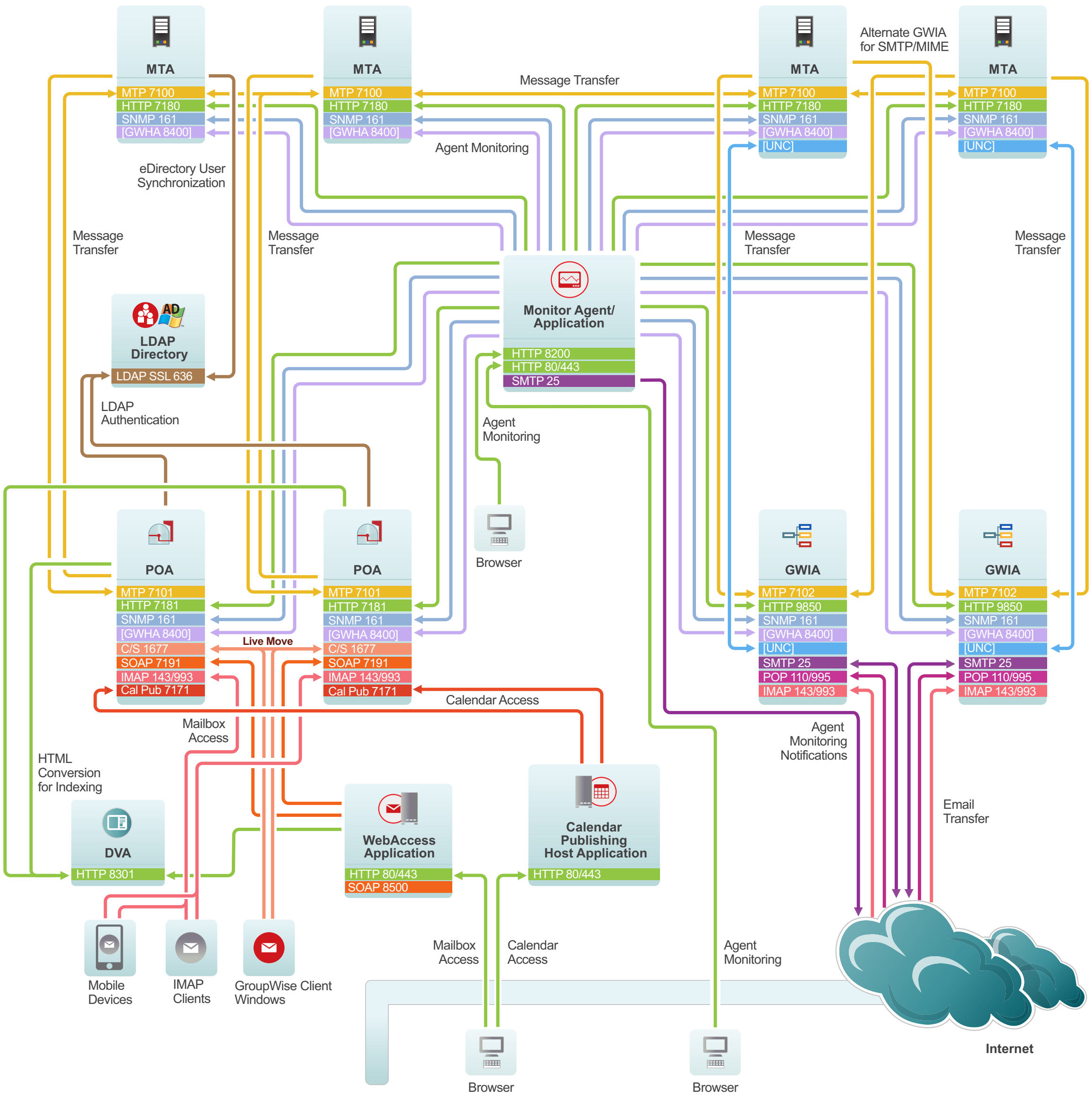
8 Accept the default of **Allow the connection**, then click **Next**.

9 Accept the default for when the rule applies, or change it depending on your security preferences for the GroupWise agents and applications, then click **Next**.

10 In the **Name** field, specify a unique name for this set of port numbers, such as `GroupWise Ports`, then click **Finish**.

Protocol Flow Diagram with Port Numbers

Click here to display a high-resolution, printable version.



See also "Port Numbers for Products Frequently Used with GroupWise" on page 731.

Post Office Agent Port Numbers

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
MTP	7101	TCP	Yes	Message Transfer Protocol Communication between the POA and the MTA
HTTP	7181	TCP	Yes	Hypertext Transfer Protocol POA console “Using the POA Console” on page 163
Internal Client/ Server	1677	TCP/ UDP	Yes	Local communication between the POA and GroupWise clients
External Client/ Server	0	TCP/ UDP	Yes	External communication between the POA and GroupWise clients (administrator-defined port number) “Securing Client Access through an External Proxy Server” on page 150
IMAP IMAP SSL	143 993	TCP/ UDP	No Yes	Internet Message Access Protocol Communication between the POP and IMAP clients such as such as Gmail and Hotmail “Supporting IMAP Clients” on page 147
SOAP	7191	TCP	Yes	Simple Object Access Protocol Communication between the POA and SOAP clients such as the GroupWise Mobility Service and Evolution “Supporting SOAP Clients” on page 148
Calendar Publishing	7171	TCP	No	Calendar Publishing Protocol Communication between the POA and the Calendar Publishing Host “Connecting the Calendar Publishing Host to a POA” and “Changing Post Office Settings” on page 625
SNMP	161	TCP/ UDP	No	Simple Network Management Protocol Communication between the POA and an SNMP management console “Using an SNMP Management Console” on page 168

Message Transfer Agent Port Numbers

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
MTP	7100	TCP	Yes	Message Transfer Protocol Communication between the MTA and the POA
HTTP	7180	TCP	Yes	Hypertext Transfer Protocol MTA console "Using the MTA Console" on page 237
SNMP	161	TCP/ UDP	No	Simple Network Management Protocol Communication between the MTA and an SNMP management console "Using an SNMP Management Console" on page 240

Internet Agent Port Numbers

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
MTP	0 or 7102	TCP	Yes	Message Transfer Protocol Communication between the GWIA and the MTA The default port number of 0 (zero) configures a direct connection between the GWIA and the MTA, rather than using TCP/IP. Port number 7102 is an example of an administrator-defined MTP port number for a TCP/IP connection.
HTTP	9850	TCP	Yes	Hypertext Transfer Protocol GWIA console "Using the GWIA Console" on page 311
SMTP	25	TCP/ UDP	Yes	Simple Mail Transfer Protocol Communication between the GWIA and email systems across the Internet Section 30, "Configuring SMTP/MIME Services," on page 293
POP POP SSL	110 995	TCP/ UDP	Yes	Post Office Protocol Communication between the GWIA POP email clients Section 31, "Configuring POP3/IMAP4 Services," on page 307

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
IMAP IMAP SSL	143 993	TCP/ UDP	No Yes	Internet Message Access Protocol Communication between the GWIA and IMAP clients such as such as Gmail and Hotmail Section 31, “Configuring POP3/IMAP4 Services,” on page 307
SNMP	161	TCP/ UDP	No	Simple Network Management Protocol Communication between the GWIA and an SNMP management console “Using an SNMP Management Console” on page 168

Document Viewer Agent Port Numbers

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
HTTP	8301	TCP	Yes	Hypertext Transfer Protocol Communication between the DVA and the POA or the WebAccess Application “Using the DVA Console” on page 373
HTTP	8302-8306	TCP	Yes	Hypertext Transfer Protocol Default DVA worker threads “Controlling Thread Usage” on page 377

WebAccess Application Port Numbers

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
HTTP	Uses Web server HTTP port	---	No	Hypertext Transfer Protocol
HTTP SSL	Uses Web server HTTPS port	---	Yes	GroupWise WebAccess user interface
SOAP	8500	UDP	No	Allow auto-update of the mailbox “Using the WebAccess Application Console” on page 621

Calendar Publishing Host Port Numbers

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
HTTP	80	TCP	No	Hypertext Transfer Protocol
HTTP SSL	443		Yes	Calendar Publishing Host user interface
				Calendar Publishing Quick Start
				Calendar Publishing Host administrator interface
				“Logging In to the CalPub Admin Console” on page 625

Monitor Agent Port Number

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
HTTP	8200	TCP	Yes	Hypertext Transfer Protocol
				Monitor Agent console
				Chapter 82, “Understanding the Monitor Agent Consoles,” on page 639

Monitor Application Port Numbers

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
HTTP	80	TCP	No	Hypertext Transfer Protocol
HTTP SSL	443		Yes	Monitor console
				Chapter 82, “Understanding the Monitor Agent Consoles,” on page 639

GroupWise High Availability Service Port Number (Linux Only)

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
HTTP	8400	TCP	No	Hypertext Transfer Protocol Communication between the Monitor Agent and the GroupWise High Availability service (gwha) (Linux only) "Configuring the Monitor Agent to Communicate with the GroupWise High Availability Service" in the *GroupWise 18 Installation Guide*

Port Numbers for Products Frequently Used with GroupWise

- "GroupWise Messenger Port Number" on page 731
- "GroupWise Mobility Service Port Numbers" on page 732
- "BlackBerry Enterprise Server for Micro Focus GroupWise Port Number" on page 732

GroupWise Messenger Port Number

Protocol	Default Port Number	TCP/ UDP	SSL Required?	Description
HTTP	8300	TCP	Yes	Communication between the Messaging Agent and Messenger clients.
HTTP	8310	TCP	Yes	Communication to the Archive Agent.
HTTP	8315	TCP	Yes	Communication between the GroupWise Admin and the Messenger Admin Rest Service.
HTTP	8320	TCP	Yes	Communication between the agents and the Messenger database.

GroupWise Mobility Service Port Numbers

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
HTTP	8120	TCP	Yes	Hypertext Transfer Protocol Mobility Admin console "Accessing the Mobility Admin Console as an Administrator" in the *GroupWise Mobility Service 18 Administration Guide*
TCP	4500	TCP	No	Proprietary TCP protocol Communication between the GroupWise Connector and the POA.
HTTP	80	TCP	No	Hypertext Transfer Protocol
HTTP SSL	443		Yes	Communication between the Mobility Connector and mobile devices

BlackBerry Enterprise Server for Micro Focus GroupWise Port Number

Protocol	Default Port Number	TCP/ UDP	SSL Available?	Description
TCP	3101	TCP	Yes	Proprietary TCP protocol Communication between BlackBerry Enterprise Server and BlackBerry devices BlackBerry Enterprise Server for Micro Focus GroupWise Administration Guide (http://docs.blackberry.com/en/admin/deliverables/20840/BlackBerry_Enterprise_Server_for_Micro Focus_GroupWise-NO_MAPTITLES_BLOBID-T813841-813841-0921092848-001-5.0.1-US.pdf)

B GroupWise URLs

Administrator URLs

In a URL, an agent server can be specified by its IP address or DNS hostname. The port numbers listed below are the default port numbers.

URL	Web Page
`http://`*mta_server*`:9710`	GW Admin Console
`http://`*poa_server*`:7181`	POA Console
`http://`*mta_server*`:7180`	MTA Console
`http://`*gwia_server*`:9850`	GWIA Console
`http://`*agent_server*`:8301`	DVA Console
`http://`*webaccess_server*`/gw/webacc/admin`	WebAccess Application Console
`http://`*monitor_server*`:8200`	Monitor Agent Console
`http://`*monitor_server*`/gwmon/gwmonitor`	Monitor Web Console
`http://`*calpubhost_server*`/gwcal/admin`	Calendar Publishing Host Admin Console

User URLs

URL	Web Page
`http://`*webaccess_server*`/gw/webacc`	WebAccess
`http://`*calpubhost_server*`/gwcal/calendar`	Calendar Publishing
`http://`*calpubhost_server*`/gwcal/freebusy/`*user_id@internet_domain*	Free/Busy Publishing

C Linux Basics for GroupWise Administration

Some GroupWise administrators might be new to the Linux operating system. This appendix provides basic Linux commands, directories, and files to assist you if are running GroupWise on Linux for the first time.

- "Linux Operating System Commands" on page 735
- "GroupWise Directories and Files on Linux" on page 738
- "GroupWise Commands on Linux" on page 740

Linux Operating System Commands

This section lists Linux commands that can help you manage your GroupWise system on Linux. It also helps you create a Linux core file if you need Support assistance with the Linux GroupWise agents.

- "Basic Commands" on page 735
- "File and Directory Commands" on page 736
- "Process Commands" on page 737
- "Disk Usage Commands" on page 737
- "Package Commands" on page 737
- "File System Commands" on page 738
- "Network Commands" on page 738
- "Linux Core File" on page 738

Basic Commands

The following basic commands are available on Linux:

Command	Description
`man` *`command`*	Displays information about any Linux command, including the commands used to start GroupWise programs.
`whoami`	Displays who you are logged in as.
`uname -a`	Displays the kernel version, along with other useful information

File and Directory Commands

The following file and directory commands are available on Linux:

Command	Description
`pwd`	Displays your current directory ("print working directory").
`ls -l`	Lists the files in the current directory, along with useful information about them.
`ls -al`	Includes hidden system files (those whose names start with a dot) in the list.
`more` *file_name*	Pages through the contents of a file (forward only).
`less` *file_name*	Pages through the contents of a file and lets you page back up through the file.
`tail` *file_name*	Displays the last 10 lines of a file. This is helpful for log files. (The `head` commands displays the first 10 lines.)
`cp` *source destination*	Copies a file or directory.
`mv` *source destination*	Moves or renames a file or directory.
`find` *starting_directory* `-name` *file_name*	Find the specified file, starting in the specified directory. Specifying / starts the find operation in the root directory.
`grep` *string file*	Searches the specified file for the specific string of characters. This is useful for locating specific information in GroupWise agent startup files.
`mkdir` *directory_name*	Creates a new directory.
`rmdir` *directory_name*	Deletes an empty directory.
`rm` *file_name*	Deletes a file.
`rm -r` *directory_name*	Deletes a directory and recursively deletes its contents.
`cat` *file_name*	Displays a file.
`cat` *file_name / printer_device*	Prints a file.

Process Commands

The following process commands are available on Linux:

Command	Description
`top`	Lists all processes, sorted by CPU percentage with the highest at the top of the list.
`ps -eaf | grep` *`program`*	Lists all processes and their IDs associated with the specified program. Wildcard characters can be used to list a group of related programs (for example, `gw*`).
`ps -aux | grep` *`user_name`*	Lists all processes and their IDs associated with the specified user.
`kill` *`process_ID`*	Stops the specified process like a normal exit.
`kill -9` *`process_ID`*	Stops the specified process after it has failed to exit normally. Temporary files are not cleaned up.
`killall` *`program`*	Kills all processes associated with the specified program.
`xkill`	Closes the window that you click on with the resulting box-shaped cursor.

Disk Usage Commands

The following disk usage commands are available on Linux:

Command	Description
`df`	Lists file system disk space usage in terms that make sense to your computer.
`df -h`	Lists file system disk space usage in terms that make sense to humans.
`du`	Lists disk space usage of each subdirectory below your current working directory
`du -s`	Lists the cumulative disk space usage of your current working directory.
`du -s` *`file_or_directory`*	Lists the disk space usage for a file or the cumulative disk space usage for a directory and its contents.

Package Commands

The following package commands are available on Linux:

Command	Description
`rpm -qa | grep novell`	Lists all Micro Focus packages installed on your server
`rpm -qi` *`package_name`*	Lists useful information about an installed package, such as name, version, release date, install date, size description, build date, and so on.
`rpm -ql` *`package_name`*	Lists where each file in the package has been installed
`rpm -e` *`package_name`*	Uninstalls a package

File System Commands

The following file system commands are available on Linux:

Command	Description
`mount`	Lists the file systems that are currently mounted on your server.
`ncpmount -S` *`fully_qualified_hostname`* `-V` *`volume_name`* `-A` *`ip_address`* `-U` *`fully_qualified_admin_user`* */linux_mount_directory*	Mounts a Linux filesystem to a Linux server.
`mount -t smbfs` *`//fully_qualified_hostname/windows_share_name`* `/linux_mount_directory` `-o username=`*`windows_administrator`*	Mounts a Windows server or Samba share as a file system on your Linux server.

Network Commands

The following network commands are available on Linux:

Command	Description
`ifconfig -a`	Lists the IP address and other detailed information about the NIC in your Linux server.
`hostname`	Displays the hostname of your server.
`dig`	Displays host information about your server
`netstat -lnp | grep` *`program`* `netstat -lnp | egrep` *`'program|program|...'`*	Lists the port numbers in use by one or more programs. It is also a handy command for checking to see whether the specified programs are currently running.
`ping` *`ip_address_or_hostname`*	Checks to see if the specified server is responding on the network.

Linux Core File

A core file is an image of a process such as a GroupWise agent that is created by the Linux operating system when the agent terminates unexpectedly. A proper core file can help Micro Focus Support determine why a GroupWise agent is having problems in your GroupWise system. See TID 3447847, "How to Obtain a GroupWise Agent Core File on Linux," in the Micro Focus Support Knowledgebase (http://www.novell.com/support/).

GroupWise Directories and Files on Linux

- "Linux Agent Software Subdirectories" on page 739
- "Linux Agent Startup and Configuration Files" on page 739

Linux Agent Software Subdirectories

The following directories contain files common to all Linux GroupWise agents:

Directory	Description
/opt/novell/groupwise/agents/bin	Executables
/opt/novell/groupwise/agents/lib	Libraries
/opt/novell/groupwise/agents/share	Startup files and language files
/etc/init.d	Startup scripts
/etc/opt/novell/groupwise	Configuration files
/var/log/novell/groupwise	Log files
/etc/sysconfig	System configuration files

Linux Agent Startup and Configuration Files

The following files are commonly used during GroupWise administration on Linux:

File	Description
/*post_office_folder*/*post_office*.poa	POA startup file
/*domain_folder*/*domain*.mta	MTA startup file
/opt/novell/groupwise/agents/share/gwdva.dva	DVA configuration file
/*domain_folder*/wpgate/gwia/gwia.cfg	GWIA configuration file
/var/opt/novell/groupwise/webaccess/webacc.cfg	WebAccess Application configuration file
/opt/novell/groupwise/agents/share/monitor.xml	Monitor Agent configuration file
/var/opt/novell/groupwise/monitor/gwmonitor.cfg	Monitor Application configuration file
/etc/xinetd.d/gwha	High Availability service definition file
/etc/opt/novell/groupwise/gwha.conf	High Availability service configuration file for controlling the agents
/etc/opt/novell/groupwise/agents/uid.conf	Non-root user configuration file
/etc/sysconfig/grpwise	Configuration options for GroupWise agents
/etc/sysconfig/grpwise-ma	Configuration options for GroupWise Monitor and GroupWise High Availability service

GroupWise Commands on Linux

Command	Description

`./grpwise start`
`./grpwise stop`
`./grpwise status`
`./grpwise print`
	Starts/stops/monitors all GroupWise agents as daemons in the `/etc/init.d` directory.

`rcgrpwise start`
`rcgrpwise stop`
`rcgrpwise status`
`rcgrpwise print`
	Starts/stops/monitors all GroupWise agents as daemons in any directory.

`rcgrpwise start` *post_office.domain*
`rcgrpwise start` *domain*
`rcgrpwise start gwdva`
`rcgrpwise` *domain*.*gwia* `start`
	Starts/stops/monitors a specific GroupWise agent as a daemon.
	Replace `start` with `stop` or `status` in any of the sample commands.

`./gwpoa --show @`*post_office*`.poa &`
`./gwmta --show @`*domain.mta* `&`
`./gwia --show @`*gwia*`.cfg &`
	Starts a specific GroupWise agent with a user interface in the `/opt/novell/groupwise/agents/bin` directory.

`./grpwise-ma start`
`./grpwise-ma stop`
`./grpwise-ma status`
 	
`rcgrpwise-ma start`
`rcgrpwise-ma stop`
`rcgrpwise-ma status`
	Starts/stops/monitors the Monitor Agent.
	The Monitor Agent does not have the same kind of user interface as the other agents. It does have a console like the other agents.